Technische Universität Darmstadt
Fachbereich Rechts- und Wirtschaftswissenschaften

Kosten von Malware und Spam

Eine empirische Untersuchung zur Zahlungsbereitschaft für IT-Sicherheit

Vom Fachbereich genehmigte Inauguraldissertation
zur Erlangung des akademischen Grades
Doctor rerum politicarum (Dr. rer. pol.)
vorgelegt von
Dipl. Wirtsch.-Inf. Oliver Schmid (geb. in Heilbronn-Neckargartach)

Referenten:
Prof. Dr. Horst Entorf (Erstreferent und Betreuer)
Prof. Dr. Ingo Barens (Korreferent)

Tag der Einreichung:
7. Dezember 2009

Tag der mündlichen Prüfung:
26. Januar 2010

Darmstadt, 2010
D17

Computer sind die Lösung auf der Suche nach Problemen.

Vorwort

Lange hat es gedauert, bis ich diese Arbeit dem Fachbereich zur Annahme vorlegen konnte, dabei stand – nicht nur in Hinblick auf diese Arbeit – nie der Gedanke im Raum, kurz vor dem Ziel noch aufzugeben, vielmehr war ich der festen Überzeugung, dass der erfolgreiche Abschluss dieses Projekts nur eine Frage der Zeit ist. Geduld ist eine Tugend, und dass ich geduldiger bin, als ich mir selbst bislang eingestehen wollte, habe ich erst in der näheren Vergangenheit erkennen dürfen.

Herzlich bedanken möchte ich mich bei meinem Doktorvater Horst Entorf, denn er hat mir nicht nur die Möglichkeit geboten, diese Arbeit anzufertigen, sondern stand mir während ihrer Entwicklung stets mit guten Ratschlägen zur Seite. Seine konstruktive Kritik und die ausführlichen Diskussionen haben maßgeblich zu meinem Verständnis für empirisches Arbeiten und dem vorliegenden Werk beigetragen. Besonderen Dank möchte ich auch Ingo Barens aussprechen, der immer großes Interesse an meiner Arbeit gezeigt hat und mich insbesondere durch sein zeitnahes Gutachten unterstützt hat. Mein spezieller Dank gilt Irene Bertschek, Margit Vanberg und Katrin Schleife vom ZEW, durch die die Durchführung der Studie erst möglich wurde, auf welcher diese Arbeit beruht. Meinen ehemaligen Kollegen Jochen Möbert, Thomas Rupp, Hannes Spengler, Emanuela Trifan und Andrea Mühlenweg danke ich für ihre fachlichen und technischen Ratschläge und die gute Zusammenarbeit am Fachgebiet. Des Weiteren erfuhr ich Unterstützung durch wissenschaftliche Hilfskräfte und Studienarbeiter, von welchen ich vor Allem Niki Becker, Daniel Langer und Lei Xuan danken möchte. Zu guter Letzt möchte ich allen anderen nicht Genannten meinen Dank aussprechen, die mich auf meinem Weg unterstützt haben.

Meinen Eltern danke ich sehr herzlich insbesondere für ihre Geduld und dafür, dass sie mich immer in dem unterstützt haben, was ich getan habe. Innigst danken möchte ich meiner Frau Deike, der wichtigsten Person in meinem Leben, die aufrichtig in guten und schlechten Zeiten auf Augenhöhe an meiner Seite steht. Ohne sie hätte ich einige Ziele nicht erreicht und wäre nicht so zufrieden mit meinem Leben. Nicht vergessen möchte ich dabei natürlich unsere Tochter Freya, welcher ich dafür danken möchte, dass sie sich mit ihrer Geburt noch bis zur Fertigstellung dieser Arbeit Zeit gelassen hat.

In der vorliegenden Arbeit habe ich versucht, mit empirischen Methoden eine Brücke zwischen Ökonomie und Informatik zu schlagen und dabei die komplexe nationale und internationale Rechtslage angemessen zu berücksichtigen. Die erwähnten gesetzlichen Vorschriften können allerdings lediglich einen Rahmen für eine auf Deutschland beschränkte Analyse bieten, da nur die relevanten Gesetze eben dieses Staats einer etwas detaillierteren Betrachtung unterzogen werden. Der Schwerpunkt der Arbeit liegt hingegen klar bei den *Kosten* von Malware und Spam und somit im Bereich der Ökonomie, aufgrund der inhaltlichen Ausrichtung ist es jedoch notwendig, einige technische Begriffe und Rahmenbedingungen im Vorfeld ausführlicher zu erläutern. Insofern mögen die einleitenden Erklärungen zunächst als recht umfangreich erscheinen, sie sind jedoch meines Erachtens nötig, um einen Überblick über den Gesamtzusammenhang bekommen zu können sowie die Wahrnehmung der Problematik in das richtige Licht zu rücken. Gerade die Veränderungen bei Schadprogrammen und unerwünschten E-Mails, aber auch in anderen Bereichen der Internet-Kriminalität scheinen in der Berichterstattung der Medien etwas zu kurz zu kommen und teilweise erst mit erheblicher Verspätung Erwähnung zu finden. Doch auch technisch interessierten Lesern soll ebenso wie Juristen durch die ausführliche Beschreibung der verwendeten Methoden die Möglichkeit geboten werden, die Vorgehensweise bei der Planung, Durchführung und Auswertung der Studie nachvollziehen zu können, da auch für sie die geschätzten Kosten von Malware und Spam von Interesse sein dürften. Unabhängig von ihrem Hintergrund wünsche ich allen Lesern eine spannende Lektüre.

Inhaltsverzeichnis

Tabellenverzeichnis

Abbildungsverzeichnis

Abkürzungsverzeichnis

IKT	Informations- und Kommunikationstechnologien
ZEW	Zentrum für Europäische Wirtschaftsforschung
CV(M)	*Contingent Valuation* (Methode)
NOAA	*National Oceanic and Atmospheric Administration*
WTP	*Willingness to pay* (Zahlungsbereitschaft)
PKS	Polizeiliche Kriminalstatistik (siehe Anhang C)
PSB	Periodischer Sicherheitsbericht
StGB	Strafgesetzbuch
UWG	Gesetz gegen den unlauteren Wettbewerb
(D)DoS	*(Distributed) Denial of Service* (siehe Glossar)
IP	*Internet Protocol* (siehe Glossar)
Anz. Antw.	Anzahl der Antworten
Anz. Beob.	Anzahl der Beobachtungen
Komm.	Kommunalität (siehe Abschnitt 3.3.1)
Korr. R^2	Korrigiertes Bestimmtheitsmaß ($\bar{R}^2$)
Max.	Maximum
Med.	Median
Min.	Minimum
MW	Mittelwert
Std. Abw.	Standardabweichung

Kapitel 1

Einleitung

Am 29. Mai 2002 verkündete FBI-Director Robert Mueller die Prioritätenliste des FBI[1], um nach Angaben der behördeneigenen Webpräsenz gegenüber „der amerikanischen Öffentlichkeit, den Strafverfolgungsbehörden und Partnern in der Geheimdienst-Gemeinschaft sowie den Mitarbeitern des FBI“ eindeutig aufzuschlüsseln, wie sich das FBI mit seinem breiten Spektrum an Aufgaben befassen will.

An dritter Stelle auf dieser Prioritätenliste steht *„Protect the United States against cyber-based attacks and high-technology crimes“*. Dabei musste der Kampf gegen *„Cybercrime“* lediglich den Aufgaben Terrorbekämpfung und Spionageabwehr weichen, die im Gegensatz zur Internet-Kriminalität eindeutig den Charakter von Geheimdiensttätigkeiten besitzen. Insofern ist die Aussage zulässig, dass die Bekämpfung der Kriminalität im *„Cyberspace“* die höchste Priorität unter den nicht-geheimdienstlichen, bundespolizeilichen Aufgaben in den Vereinigten Staaten von Amerika erlangt hat.

Seine Aufgaben im Bereich der Internet-Kriminalität beschreibt das FBI auf seiner *„Cyber Investigations“*-Webseite folgendermaßen:

„The FBI's cyber mission is four-fold: first and foremost, to stop those behind the most serious computer intrusions and the spread of malicious code; second, to identify and thwart online sexual predators who use the Internet to meet and exploit children and to produce, possess, or share child pornography;

[1] Das ***F****ederal* ***B****ureau of* ***I****nvestigation* ist eine US-amerikanische bundespolizeiliche Ermittlungsbehörde und entspräche in Deutschland am Ehesten dem Bundeskriminalamt.

third, to counteract operations that target U.S. intellectual property, endangering our national security and competitiveness; and fourth, to dismantle national and transnational organized criminal enterprises engaging in Internet fraud. Pursuant to the National Strategy to Secure Cyberspace signed by the President, the Department of Justice and the FBI lead the national effort to investigate and prosecute cybercrime.“

An erster Stelle steht mit ausdrücklichem Vorrang die Jagd nach den Tätern in den gravierendsten Fällen von unberechtigtem Eindringen in Computersysteme *(„intrusion“)* sowie die Verfolgung derjenigen Kriminellen, die schädlichen Code verbreiten, also Viren, Würmer und Trojaner programmieren. Des Weiteren will das FBI verstärkt gegen die Verbreitung von Kinderpornographie im Internet vorgehen, Gegenmaßnahmen zu Angriffen auf die Nationale Sicherheit einleiten sowie den Betrug im Internet bekämpfen. Während der erste und dritte Punkt der Aufzählung auf kriminelle Handlungen abzielen, die von der Existenz von Computern bzw. dem Internet abhängig sind, handelt es sich bei Betrug und dem Verbreiten von illegaler Pornographie um Delikte, welche es schon von der Entstehung des weltweiten Datennetzes gab.

In den letzten Jahren häuften sich in der Berichterstattung der Medien die Meldungen über die Verbreitung von illegalen Kopien von Programmen, Filmen und Musik, von Kinderpornographie und extremistischer Propaganda. Diese Gruppen von Straftaten, welche das Internet als neuen Verbreitungsweg für sich entdeckt haben, auf dieses Medium aber für die Durchführung der strafbaren Handlung nicht zwingend angewiesen sind, werden in der vorliegenden Arbeit nicht weiter betrachtet. Durch das Internet ist es für die Täter zwar erheblich einfacher geworden, bei (vermeintlicher) Wahrung der Anonymität einem größeren Kreis potentieller Interessenten die illegalen Waren oder Dienstleistungen einfacher und schneller anbieten zu können und zukommen zu lassen. Doch schon vor den 90er Jahren, in denen das Internet den ersten Privatpersonen zugänglich gemacht wurde, war die Verbreitung des illegalen Materials möglich, auch wenn es für Kaufinteressenten mit einem größeren Aufwand verbunden war und ihre Anonymität wiederum nicht gewahrt blieb.

Betrügerische Handlungen haben durch das Internet mit der Entwicklung innovativer Methoden neue Facetten hinzugewonnen, aber auch teilweise alte Ideen neu aufgegriffen. Eine Form des Vorschussbetrugs ist der „Nigerianische Brief“[2], in welchem dem potentiellen Opfer per E-Mail die hohe Vergütung eines zu leistenden Vorschusses versprochen wird, mit dessen Hilfe ein immenses Vermögen außer Landes geschafft werden soll. Diese früher auch per Fax verbreitete Nachricht sprach häufig von den Anwaltskosten für eine hohe Erbschaft in Nigeria, woher anfangs auch die meisten Täter dieses Betrugsversuchs stammten, inzwischen variieren die Herkunftsländer jedoch. Sollten die Gebühren nicht bis zu einem Stichtag entrichtet worden sein, so sollte das Vermögen dem Staat zufließen, was den Urheber der Nachricht dazu veranlasst habe, den „als vertrauenswürdig bekannten“ Empfänger zu kontaktieren. Bezahlte das „eher vertrauensselige“ Opfer die Summe, wurde häufig noch die Begleichung weiterer Kosten erbeten, bis sich entweder die Betrüger nicht mehr meldeten oder das Opfer die Zahlungen einstellte.

Die Beschwerden über Betrug im Internet haben in den Vereinigten Staaten nach Angaben des *Internet Crime Complaint Center (IC3)*[3] (2007) im Zeitraum zwischen 2000 und 2005 stark zugenommen, bevor diese Zahl im Jahr 2006 erstmals leicht zurückging, der Schwerpunkt liegt mit nahezu der Hälfte der Fälle bei Betrug mit Internet-Auktionen.

In der deutschen Rechtsprechung wird bei solchen Betrugsdelikten gemäß Strafgesetzbuch (StGB) zwischen Betrug (im Allgemeinen) nach § 263 StGB und Computerbetrug nach § 263 a StGB unterschieden. Dabei ist der Passus „das Ergebnis eines Datenverarbeitungsvorgangs [...] beeinflusst“ ausschlaggebend dafür, dass ein Betrugsdelikt als Computerbetrug angesehen wird. Dieser Fall tritt jedoch im Zusammenhang mit Internet-Auktionen nur dann ein, wenn eine technische Manipulation beispielsweise der Webseite vorlag, bei einer Nichtlieferung der Ware hingegen handelt es sich um Betrug im herkömmlichen Sinn, so dass § 263 a StGB nicht greift.

---

[2] Die Betrugsmasche ist auch unter dem Namen *„Nigeria-Connection“* bekannt.

[3] Das ***I****nternet* ***C****rime* ***C****omplaint* ***C****enter* ist ein Projekt des FBI und des *National White Collar Crime Center (NW3C)* zur Koordinierung von Beschwerden über Internet-Kriminalität. Es nahm seine Arbeit am 8. Mai 2000 als *Internet Fraud Complaint Center (IFCC)* auf und wurde im Dezember 2003 umbenannt.

Bei Betrug im Internet handelt es sich somit häufig um Delikte, welche den Computer bzw. das Internet als Medium nutzen, um die Straftat beispielsweise anonym oder unter falschen Angaben begehen zu können. Diese Delikte werden daher in die vorliegende Arbeit ebenfalls nicht weiter einbezogen, da das neue Medium nicht zwingend notwendig wäre, um ein strafbares Handeln zu ermöglichen.

Der „Erste Periodische Sicherheitsbericht“ (2001)[4] spricht im Zusammenhang mit diesen Straftaten von „Delikten, bei denen das Internet als virtuelles Tatwerkzeug [...] genutzt wird“, und unterscheidet sie von „Straftaten, die das Internet einschließlich der angebotenen Dienste Angriffen aussetzen oder das Internet nutzen, um Angriffe auf die Sicherheit, Zuverlässigkeit und Integrität von Daten auszuführen“. Während die erstgenannten Delikte in der vom Bundeskriminalamt (BKA) jährlich veröffentlichten „Polizeilichen Kriminalstatistik“ nicht getrennt ausgewiesen werden, wird der Bereich der Computerkriminalität als eigenständige Straftatengruppe geführt. Den quantitativen Schwerpunkt bildet dabei der „Betrug mittels rechtswidrig erlangter Debitkarten mit PIN“[5], welcher aktuell etwa die Hälfte der erfassten Delikte ausmacht, im Jahr 2002 sogar noch fast zwei Drittel.

Der tatsächliche Computerbetrug nach § 263 a StGB machte im Jahr 2006 ungefähr ein Viertel der Computerkriminalität aus, die weiteren Deliktsarten weisen relativ geringe Fallzahlen auf (siehe Anhang C). Diese Zahlen müssen jedoch unter dem Vorbehalt gesehen werden, dass laut PSB (2001) „von einem extrem großen Dunkelfeld ausgegangen werden muss“, so dass die Kriminalstatistiken nur die Spitze des Eisbergs zeigen. Gestützt wird diese Annahme durch die Angaben des Ersten Periodischen Sicherheitsberichts, dass es in Deutschland im Jahr 2000 durch den *„I love you“*-Wurm bei 21 % der mit Computern ausgestatteten Arbeitsplätze zu Behinderungen und Arbeitsausfällen kam, dem BKA bei der Veröffentlichung des PSB aber lediglich vier Anzeigen wegen Computersabotage vorlagen.

[4] Im 2006 erschienenen „Zweiten Periodischen Sicherheitsbericht“ wird im Bereich Internet-Kriminalität lediglich auf Kinderpornographie, Extremismus und Terrorismus sowie Betrug eingegangen. Das Thema Malware wird hingegen überhaupt nicht berücksichtigt, Spam nur im Zusammenhang mit der Verbreitung extremistischer Propaganda.

[5] Bis 2001 „Betrug mittels rechtswidrig erlangter Karten für Geldausgabe- bzw. Kassenautomaten“.

Die Kosten, die durch einen solchen Malware-Vorfall verursacht werden, sind vielfältig und nur teilweise messbar. Neben dem reinen Produktivitätsverlust durch Ausfallzeiten von einzelnen Rechnern oder ganzen Computersystemen sowie den Investitions- und Personalkosten für IT-Sicherheit spielen vor Allem Imageverluste betroffener Unternehmen eine große Rolle. In diesem Risiko, wegen (möglicher) Mängel in der IT-Sicherheit Kunden zu verlieren, sehen auch die Autoren des Periodischen Sicherheitsberichts einen wichtigen Grund für die geringe Anzeigebereitschaft und somit implizit für das Dunkelfeld. Die Folgen von Problemen mit Malware gehen aber bis hin zu Vertrauensverlusten in die Computertechnik und spielen so beispielsweise auch bei der Nutzung von E-Mail und der damit verbundenen Bekämpfung von Spam durch Filtermaßnahmen eine arbeitspsychologische Rolle.

Die Angaben zu „Schäden“, welche durch einen Virus oder einen Wurm verursacht wurden, müssen jedoch häufig kritisch betrachtet werden und halten dann oft dieser Inaugenscheinnahme nicht stand. Dabei ist meistens nicht die Glaubwürdigkeit der Quelle das Problem, sondern eine mangelnde Aufschlüsselung der betrachteten Kostentreiber oder teilweise einfach nur unpräzise Angaben. So bezifferte das Bundesamt für Sicherheit in der Informationstechnik (BSI) in seiner Viren-Chronik (2009) den durch *„Code Red“* im Jahr 2001 verursachten Schaden auf zwei Milliarden US-Dollar. Andere Quellen wie beispielsweise Computerwoche.de (2001) berichteten hingegen unter Berufung auf das US-amerikanische Marktforschungsunternehmen *Computer Economics* von 2,6 Milliarden US-Dollar, je nach Quelle variieren die veröffentlichten Werte zwischen 1,2 und 8,7 Milliarden US-Dollar. Mit Ausnahme von *Computer Economics* schlüsselte jedoch keine Quelle genauer auf, aus welchen Kosten sich die Summe zusammensetzt, teilweise wurde nicht einmal angegeben, ob sich der Wert auf die weltweiten Kosten bezieht oder ob nur eine Region wie Nordamerika oder Europa betrachtet wurde.

Die Kosten durch Produktivitätsausfälle beliefen sich laut Computerwoche.de auf ungefähr 1,5 Milliarden, während die Bekämpfung des Wurms Kosten von 1,1 Milliarden verursachte, darunter das Testen, Säubern und *„Patchen“* (vom englischen „(aus-)flicken“, „reparieren“) der Systeme. Die Software zum Schließen der Sicherheitslücke stand jedoch schon einen Monat vor dem ersten Auftreten des Schadprogramms auf der Webseite von Microsoft

zur Verfügung, so dass die Infektion durch das präventive Patchen hätte verhindert werden können. Insofern ist fraglich, inwiefern die korrektive Installation wirklich zu den Kosten durch den Wurm gerechnet werden darf, und ob nicht vielmehr ein Großteil der Kosten durch Versäumnisse in der Systempflege begründet sind. Nach Angaben von Microsoft (2004) lagen in der Vergangenheit zwischen der Veröffentlichung eines Patches und dem Erscheinen von Schadprogrammen, welche die zu schließende Lücke nutzten, teilweise Monate, wenn auch mit stark sinkender Tendenz.[6] Demnach sollte es oft im Vorfeld einer „Viren-Epidemie“ möglich sein, sich durch präventive Maßnahmen gegen die Schadprogramme zu schützen. Außer Frage steht indes, dass die Kosten für das Schließen von Sicherheitslücken zumindest teilweise jenen Kosten zugerechnet werden können, die durch Schadprogramme, also Viren, Würmer und Trojaner, verursacht werden.

Werden Unternehmen befragt, wie hoch sie die „Schäden“ schätzen, die ihnen durch Schadprogramme entstanden sind, so wäre es durchaus möglich, dass die Angaben auf Basis jener Kosten gemacht werden, die beispielsweise durch die Beseitigung eines Virus aus dem System entstanden sind. Doch spätestens bei der nicht näher präzisierten Frage nach den „Kosten“ werden die Angaben divergieren, da manche Unternehmen beispielsweise die Personalkosten für Administratoren berücksichtigen, andere hingegen die Meinung vertreten, diese Fachkräfte würden ohnehin beschäftigt, auch ohne konkrete Vorfälle. Auch bleibt in diesem Zusammenhang offen, ob bei der direkten Frage nach den entstandenen Kosten die Angaben zu eventuellen Vorfällen mit Schadprogrammen beschönigt werden oder Vorkommnisse völlig verschwiegen werden.

Diesen Eindruck bestätigen die <kes>-Studien aus den Jahren 2004 und 2006, in der jüngeren Studie wurde sogar die Aussage getroffen „Auch mit Schätz- oder Erfahrungswerten zu Ausfallzeiten und Kosten taten sich die meisten Befragten schwer [...]“. So hatte die Frage zu durch Malware-Infektionen verursachten Ausfallzeiten und Kosten nur gut jedes dritte teilnehmende Unternehmen beantwortet, bei den weiteren Sicherheitsvorfällen sank dieser Anteil sogar auf ein Sechstel, auch unterlagen die angegebenen Werte zum Teil stärkeren Schwankungen.

[6] Nicht immer erscheinen die Patches vor den dazugehörenden Schadprogrammen, so dass ein regelmäßiges Patchen der Systeme keine Sicherheitsgarantie darstellt.

Im Rahmen der vorliegenden Arbeit wurde in Zusammenarbeit mit dem Zentrum für Europäische Wirtschaftsforschung (ZEW) in Mannheim eine Unternehmensbefragung zur Feststellung der Kosten von Schadprogrammen durchgeführt. Dabei wurde die Studie auf die sogenannte *„Contingent Valuation Method“* ausgerichtet, bei welcher nicht nach durch Schadprogramme verursachten Kosten gefragt wird, sondern die Zahlungsbereitschaft zur Bekämpfung von Viren und Würmern erfragt wird. Weiterhin wurden die Unternehmen gebeten, eine Zahlungsbereitschaft zur Eindämmung der Spam-Problematik zu äußern, da dieses Phänomen im E-Mail-Alltag zwar nicht direkt als Bedrohung zu sehen ist, aber als eine Belästigung, die in gewissem Maße ebenfalls die Gewährleistung der IT-Sicherheit einschränkt.

In Kapitel 2 werden die Grundlagen für die vorliegende Arbeit entwickelt, dabei wird zunächst ein kurzer Einblick in die komplexen Themengebiete Malware und Spam gegeben sowie der Zusammenhang zwischen den beiden Arten von Internet-Kriminalität aufgezeigt. Danach folgt ein Überblick über den Stand der Forschung im Bereich der Kostenquantifizierung dieser Bedrohungen für die IT-Sicherheit, für welchen von mehreren Wissenschaftlern ein Nachholbedarf konstatiert wird. Zuletzt werden in den theoretischen Überlegungen eigene Hypothesen zu den Kosten von Malware und Spam sowie ihrer Schätzung entwickelt.

Eine kurze Beschreibung verschiedener Bewertungsansätze leitet Kapitel 3 ein, danach wird die Entscheidung für die Wahl der sogenannten *Contingent Valuation* Methode begründet und die Vor- und Nachteile des Konzepts diskutiert. An dieser Stelle werden auch die bisherigen Studien zu Kosten von Kriminalität unter Anwendung dieser Methode betrachtet. Darüber hinaus wird ein kurzer Überblick über die eingesetzten Methoden zur Schätzung der aus der Umfrage resultierenden Ergebnisse gegeben.

Die Datenbasis, auf welcher die vorliegende Arbeit beruht, wird in Kapitel 4 vorgestellt. Dabei handelt es sich um einen Datensatz zur Zahlungsbereitschaft für IT-Sicherheit, welcher in Zusammenarbeit mit dem ZEW erhoben wurde und den Analysen in Kapitel 5 zugrunde liegt. Dieses Kapitel behandelt die Zahlungsbereitschaft von Unternehmen für die Reduzierung von Malware und Spam, indem zunächst die Ergebnisse der deskriptiven Analyse vorgestellt werden, bevor die Faktorenanalyse mögliche Zusammen-

hänge zwischen einzelnen Variablen aufdeckt. In den Regressionsanalysen werden die Zahlungsbereitschaften der Unternehmen für die beiden fokussierten Bereiche der IT-Sicherheit geschätzt, außerdem werden die wichtigsten Einflussfaktoren für Vorfälle mit Schadprogrammen sowie Belästigung durch Spam-Mails präsentiert. Im Anschluss folgen weitere Regressionsergebnisse, die im Zusammenhang mit der Studie entwickelt wurden. Die Bemerkungen in Kapitel 6 schließen die Arbeit ab.

Kapitel 2

Grundlagen

Als Bill Gates im Januar 2004 einen Blick in die Zukunft wagte, hatte er die Rechnung ohne die Spammer gemacht. *„Two years from now, spam will be solved“* verkündete er gemäß CBS NEWS (2004) einer ausgewählten Teilnehmergruppe auf dem *World Economic Forum* in Davos (Schweiz). Dass die Realität anders aussieht, zeigt sich vier Jahre nach der visionären Überwindung der Spam-Problematik bei einem Blick in die Mailbox.

Tatsache ist, dass sich die Spam-Situation seit dieser Aussage weltweit kontinuierlich verschlechtert hat, besonders Unternehmen, die als Mail-Provider tätig sind, sehen sich tagtäglich mit einer immer größeren Flut von Spam-Mails konfrontiert. Doch nicht nur Kommunikationsdienstleister sehen sich gezwungen, sich gegen das steigende Spam-Aufkommen zu wappnen, heutzutage müssen im Prinzip alle Unternehmen in den Schutz vor Spam-Mails investieren. Diese Schutzmaßnahmen verursachen Kosten, ebenso wie diejenigen Spam-Mails, die nicht von Spam-Filtern identifiziert werden konnten und durch verlorene Arbeitszeit zu Produktivitätseinbußen führen.

Doch eine noch größere Kostenquelle stellen Schadprogramme dar, da sie neben höheren Kosten für Schutzmaßnahmen im Falle eines Misserfolgs auch ein erheblich größeres Schadens- und damit Kostenpotential besitzen. Die möglichen Folgen eines Malware-Vorfalls sind ebenso breit gefächert wie die Spanne der durch sie verursachten Kosten, jene Kosten zu quantifizieren stellt jedoch aus verschiedenen Gründen ein großes Problem dar, wie das folgende Kapitel zeigen wird.

Bevor jedoch ein Überblick über die bisherigen Studien zur Schätzung solcher Kosten gegeben wird, müssen die komplexen Themengebiete der Schadprogramme auf der einen Seite und der unerwünschten E-Mails auf der anderen Seite kurz beleuchtet werden. Beide Phänomene haben in der vergangenen Dekade eine erhebliche Entwicklung durchgemacht, welche der Grund dafür ist, dass Malware und Spam in dieser Arbeit gemeinsam betrachtet werden. Zunächst erfolgt ein Abriss der Entwicklung über einen Zeitraum von 60 Jahren hinweg von der theoretischen Idee eines Wissenschaftlers bis zur alltäglichen Bedrohung eines jeden Computerbesitzers. Den Schwerpunkt dieses Ausflugs in die Geschichte der Malware bildet eine Beschreibung der für die vorliegende Arbeit relevanten Veränderungen sowie des Status quo. Das inzwischen für jeden E-Mail-Nutzer fast unumgängliche Problem der unerwünschten E-Mails wird im Anschluss behandelt, auch hier liegt der Fokus auf den zum weiteren Verständnis notwendigen Fakten. Dabei wird zunächst versucht, den Begriff „Spam“ zu definieren, bevor seine Geschichte in Kürze beleuchtet wird und die Spam-Mails mit Schadprogrammen in Zusammenhang gebracht werden.

2.1 Technische Hintergründe

Die IT-Sicherheit wird durch zahlreiche Bedrohungen beeinträchtigt und ist ständig neuen Gefahren ausgesetzt, dies gilt sowohl für private Nutzer als auch für Unternehmen. Der <kes>-Studie (2006a) nach zu urteilen, sahen die meisten der teilnehmenden Unternehmen Irrtum und Nachlässigkeit der eigenen Mitarbeiter als größte aktuelle Bedrohung an und prognostizierten für Malware den Aufstieg vom zweiten Platz zur bedeutendsten Gefahr für die IT-Sicherheit. Mit geringerer Priorisierung folgen auf den Plätzen Mängel und Defekte in den Bereichen Soft- und Hardware, deren Ausfälle nach eigenen Angaben in fast der Hälfte der Unternehmen „Schäden“ verursacht hat, genau wie ungewollte Fehler der Mitarbeiter. Im Gegensatz dazu gab nur jedes dritte Unternehmen an, durch Schadprogramme verursachte Kosten beklagen zu müssen, doch trotz eines Rückgangs der Vorfälle verursachten Viren, Würmer und Trojaner die größten Schadensereignisse bei den beobachteten Unternehmen.

Das Problem der Spam-Mails, das möglicherweise von vielen Unternehmen nicht als Bedrohung identifiziert wird, ist in der Auflistung der aktuellen sowie der zu erwartenden Gefahren nicht geführt. Tatsächlich wurde Spam lange Zeit nur als Belästigung angesehen, durch das enorme Spam-Aufkommen wird hierdurch jedoch inzwischen die Verfügbarkeit von Servern stark eingeschränkt, durch den notwendig gewordenen Einsatz von Filtermaßnahmen ist in der Zwischenzeit auch die Verfügbarkeit und Integrität der E-Mails beeinträchtigt. Während die unerwünschten E-Mails gemäß der <kes>-Studie (2006a) vermutlich von vielen Unternehmen bislang nur als störend angesehen werden, bezeichnete Robert Rothe, der Gründer des E-Mail-Security-Unternehmens *eleven,* auf dem *5th German Anti-Spam Summit* (2007) Spam als „eine permanente *Denial of Service*-Bedrohung“[1].

2.1.1 Schadprogramme (Malware)

Als Schadprogramme oder Malware[2] werden Computerprogramme[3] bezeichnet, welche vom Benutzer ungewollte Funktionen besitzen und diese zumeist ohne Wissen des Benutzers ausführen. Häufig wird im allgemeinen Sprachgebrauch im Zusammenhang mit Schadprogrammen auch von Viren gesprochen, ohne damit explizit den Malware-Typ „Virus“ zu meinen, sondern um das Wort als Oberbegriff für Viren, Würmer und „Trojaner“ zu verwenden. Durch diese Angewohnheit lässt sich auch erklären, warum die Schutzprogramme üblicherweise als Anti-Viren-Programme bezeichnet werden und nicht als Anti-Malware-Programme.

Doch nicht bei allen Phänomenen, welche mit Malware in Verbindung gebracht werden, handelt es sich wirklich um Schadprogramme, sondern teilweise wie im Fall der *„Hoaxes“* auch lediglich um E-Mails, welche durch ihren Inhalt schädlichen Charakter haben. Im Übrigen bezeichnet Malware keine fehlerhaften Programme, auch wenn diese tatsächlich Schaden anrichten (können), sondern nur Software, die von ihrem Entwickler mit einer dem

[1] *„Spam has turned into a permanent DOS menace.“* [sic!].

[2] Das englische Kofferwort ist zusammengesetzt aus *„**mal**icious“* (bösartig, arglistig) und *„soft**ware**“*.

[3] Der Vollständigkeit halber sei an dieser Stelle erwähnt, dass es inzwischen auch die ersten Schadprogramme für Mobiltelefone gibt.

Benutzer vorsätzlich verheimlichten Funktion versehen worden ist.

Als im März 1992 der Virus *Michelangelo* erstmals ausbrach und eine Viren-Hysterie verursachte, wurden sich die Medien zum ersten Mal der Gefahr von Schadprogrammen bewusst und berichteten zunächst umfangreich von dem Ereignis. Dabei blickte man zu diesem Zeitpunkt schon auf zwei Jahrzehnte der praktischen Malware-Entwicklung zurück, die theoretischen Grundlagen waren bereits mehr als doppelt so alt. Noch vor wenigen Jahren verging kaum ein Monat, in dem keine Meldungen von neuen Schadprogrammen veröffentlicht wurden, die mit innovativen Veränderungen die Internet-Gemeinschaft in Atem hielten. Inzwischen steigt die Anzahl neuer Malware-Exemplare zwar unvermindert weiter, um die technischen Weiterentwicklungen ist es hingegen etwas stiller geworden.

Die theoretischen Grundlagen gehen auf den Mathematiker John von Neumann zurück, der im Jahr 1949 seine Arbeit *„Theory and Organization of Complicated Automata“* vorstellte. In ihr und dem unvollendeten Manuskript *„The Theory of Automata: Construction, Reproduction, Homogeneity“* erläuterte von Neumann seine Idee, wie sich Computerprogramme selbst reproduzieren können, der Mathematiker Lionel Penrose vertiefte die Idee 1959 in seinem Artikel *„Self-Reproducing Machines“*. Dort beschrieb er ein einfaches Modell ähnlicher Struktur, welches die Fähigkeiten besaß, aktiviert zu werden, sich zu multiplizieren, zu mutieren und anzugreifen, die praktische Umsetzung dieses theoretischen Vorschlags erfolgte gemäß Kaspersky (2003) kurz darauf durch Frederick Stahl.

Als erster Virus wird häufig der *Creeper* angesehen, der Anfang der 70er Jahre im ARPANET[4] auftauchte. Das Programm verbreitete sich unter dem Betriebssystem Tenex per Modem auf andere Computer und gab auf befallenen Rechnern den Text *„I'm the Creeper: Catch me if you can.“* (in Großbuchstaben) aus. Bald darauf erschien mit dem *Reaper* ein Programm, welches in der Lage war, sich innerhalb des Netzwerkes zu verbreiten, den *Creeper* aufzuspüren und aus dem System zu entfernen.

[4]Das ***A****dvanced* ***R****esearch* ***P****rojects* ***A****gency* ***Net****work* war ein Computernetzwerk zur Verbindung US-amerikanischer Universitäten, die im Auftrag des US-Verteidigungsministeriums forschten. Das Computernetz der Militärforscher gilt als der Vorläufer des Internets.

Mit dem *Elk Cloner* zeigte sich bereits 1982 eine wichtige Voraussetzung für Malware, von der Verbreitung eines Betriebssystems war abhängig, wie viele Schadprogramme dafür geschrieben wurden. Der Bootvirus wurde für den damals weit verbreiteten Apple II geschrieben und duplizierte sich über den Bootsektor infizierter Floppy-Disks, auf denen damals noch das Betriebssystem gespeichert wurde. Bei jedem fünfzigsten Bootvorgang wurde der Virus aktiviert und gab ein Gedicht auf dem Bildschirm aus, negative Effekte hatte der Virus damals nicht für die überraschten und ahnungslosen (privaten) Computerbesitzer, welche damit erstmals mit einem Virus außerhalb von Forschungsnetzen konfrontiert wurden.

Der Begriff des „Virus“ wurde aber erst im Jahr 1983 geprägt, als Frederick Cohen am 10. November im Rahmen seiner Dissertation an der Lehigh Universität (Pennsylvania) ein sich selbst reproduzierendes Programm namens *„V“* vorstellte. Ein Jahr darauf sprach Cohen auf Vorschlag seines Lehrers Prof. Leonard M. Adleman von einem „Computervirus“ sowie der Infektion anderer Programme und definierte 1984 in *„Computer Viruses – Theory and Experiments“* die grundlegenden Eigenschaften eines Virus.

Als im Jahr 1987 ein Virus für Macintosh-Computer entdeckt wurde, zeigte sich die Unerfahrenheit der Branche mit dem langsam auftretenden Problem, so lieferte Apple seine Betriebssysteme umgehend mit einem Viren-Suchprogramm aus – das genau diese eine Virenfamilie aufspüren konnte, aber keine weiteren. Im gleichen Jahr konnte im Kampf gegen Viren ein erster Erfolg verbucht werden, als zum ersten Mal ein IBM-kompatibler Virus neutralisiert werden konnte.

Entscheidend für die weitere Entwicklung der Malware war *Cascade,* dessen Erscheinungsbild sich aufgrund seiner Verschlüsselungsroutine mit jeder Infizierung änderte, weswegen er als Vorläufer der polymorphen Viren angesehen werden kann. Benannt wurde der Virus, welcher auch unter dem Namen *Falling Letters* bekannt ist, nach seiner Schadroutine, welche nach seiner Aktivierung die Zeichen des Textes in Kaskaden den Bildschirm hinabfallen ließ. Waren bis dato die Schadensroutinen zumeist eher als harmlos zu bezeichnen, tauchten im Jahr 1987 aber auch die ersten Viren auf, welche beispielsweise ausgelöst durch das aktuelle Datum des Computers (mehr oder weniger umfangreich) Daten löschten.

Mit der Durchsetzung der IBM-kompatiblen PCs erschienen bereits Mitte der 80er zunehmend Viren für diese Geräte, und durch die neu aufkommenden Schadprogramme mit Löschfunktion wurden sich Firmen mit Computerarbeitsplätzen sowie interessierte private Computernutzer dieser Gefahr bewusst. In den kommenden Jahren wurden vermehrt Unternehmen gegründet, die mit wenigen Mitarbeitern Anti-Viren-Software produzierten, in der Anfangszeit verlief die gesamte Entwicklung aber noch recht langsam. So waren Computer noch nicht sehr oft in Büros oder gar privaten Haushalten anzutreffen, der Datenaustausch zwischen Computern erfolgte häufig noch über (360 k-)Disketten[5], und Updates mit neuen Malware-Definitionen wurden noch, von manchen Anbietern einmal monatlich, auf Diskette per Post verschickt. Dabei war diese Verbreitungsgeschwindigkeit zum damaligen Zeitpunkt durchaus nicht unangemessen, wie sich am Beispiel der Ausbreitung des Virus *AntiCMOS* alias *Lenart* zeigen lässt. So tauchte der Virus Anfang 1994 erstmals im slowenischen Städtchen Lenart auf, in Nordamerika hingegen fand er erst im Frühjahr 1995 größere Verbreitung.

Im August 1995 läutete *Concept* mit den Makroviren, welche zunächst nur die Makros von Word-Dokumenten, später die Dateien aller Office-Anwendungen infizierten, eine neue Generation von Malware ein. Anfang der 90er war die Weitergabe von infizierten Datenträgern noch der vornehmliche Verbreitungsweg von Schadprogrammen, da durch die geringe Verbreitung des Internets eine Ausbreitung über das Datennetz nur eingeschränkt möglich war. Das Internet-Zeitalter begann für Viren und Würmer mit dem Jahr 1997, als *ShareFun* als erster (Makro-)Virus mit MS Mail den Weg der E-Mail nutzte. Am 26. März 1999 wurde einer breiten Öffentlichkeit die Bedrohung durch Malware vor Augen geführt, als sich der E-Mail-Wurm *Melissa* in bislang nie dagewesener Geschwindigkeit verbreitete und sogar Unternehmen wie Intel und Microsoft dazu zwang, ihre Mail-Server vorübergehend herunterzufahren. Der Makrovirus verschickte sich nach der Infektion umgehend an die ersten 50 Einträge des Adressbuchs von MS Outlook 97 bzw. 98 und war somit das erste prominente Schadprogramm, welches die Verbreitung dieser Versionen

[5]Das Datenvolumen von 360 Kilobyte entspricht einem Viertel der Kapazität von heute teilweise noch verwendeten 1,44 MB-Disketten. Zum Vergleich verfügen heutzutage handelsübliche CDs über 650-700 MB und DVDs über 4,7 GB.

des Mail-Programms für seine eigene Ausbreitung nutzte. Bereits zwei Monate zuvor hatte sich *Happy99* auf die gleiche Weise verbreitet und mit einem Feuerwerk auf dem Bildschirm seines Opfers als Neujahrsgruß getarnt, das Ausmaß der Verbreitung stand aber in keinem Vergleich zu *Melissas* zweifelhaftem Erfolg.

Das neue Jahrtausend begann verhältnismäßig ruhig, war doch ein großer Blackout durch die Datumsumstellung und den damit verbundenen *Y2k-Bug*[6] befürchtet worden. Diese Stille hielt bis zum 4. Mai an, als viele E-Mail-Leser von einem unerwarteten Liebesbrief mit der Betreffzeile „I love you“ überrascht wurden. Wieder einmal machte sich mit *LoveLetter* ein Wurm das Adressbuch von Outlook zunutze, um sich per E-Mail zu versenden, im Gegensatz zu *Melissa* an alle Einträge. Dabei spekulierte das Schadprogramm auf die Neugier der Empfänger, welche dem Hinweis auf den Liebesbrief im Anhang folgen sollten, um die vermeintliche Textdatei `LOVE-LETTER-FOR-YOU.TXT.vbs` zu öffnen und damit ein Skript zu aktivieren. Nach der Infektion verschickte sich der E-Mail-Wurm weiter und löschte alle Dateien mit bestimmten Dateiendungen, um sie mit einer Kopie seiner selbst unter gleichem Namen zu ersetzen.[7] Da Skript-Programme von vielen Experten bis dahin unterschätzt worden waren, übertraf *LoveLetter* sogar die Verbreitung von *Melissa,* infolge der Epidemie sahen sich zahlreiche Unternehmen gezwungen, ihre E-Mail-Server vom Netz zu nehmen.

Das Jahr 2000 war das erste, in dem sich Würmer hauptsächlich per E-Mail verbreiteten, nach Angaben von Kaspersky (2003) erfolgten ca. 80 % aller Infektionen per E-Mail, ein Anteil, welcher sich im Folgejahr auf fast 90 % erhöhen sollte. Auch wurden ab dieser Zeit die Internet-Würmer immer vielseitiger, so gingen als *„Harvester“* bezeichnete E-Mail-Würmer nun vermehrt dazu über, sich nicht mehr nur der Adressbücher der infizierten Rechner zu bedienen, sondern den Rechner regelrecht nach Adressen zu durchsuchen. Außerdem begannen die Würmer, sich mittels einer eigenen *SMTP-Engine*

[6] *Y2k* steht für ***Y****ear* ***2000;*** es wurde befürchtet, dass Soft- und Hardware, Telekommunikations- und Transportsysteme, Anlagensysteme und sogar medizinische Geräte durch Fehler in der Jahresumstellung fehlerhaft oder überhaupt nicht mehr funktionieren.

[7] Lediglich die Dateiendung `.vbs` wurde angehängt, sofern die ersetzte Datei nicht schon eine entsprechende Skriptdatei war.

zu verbreiten, wodurch sie nicht mehr auf Programme wie Outlook angewiesen waren, oft fälschten sie den Absender und wählten aus ihren Texten teilweise sogar die Sprache, welche zu der Länderkennung der Empfängeradresse passte.

Ab 2001 nutzte eine wachsende Anzahl an Würmern Sicherheitslücken auf Microsoft-Rechnern, um sich zu verbreiten, beispielsweise das automatische Öffnen von an E-Mails angehängten Dateien durch Outlook, und jene Programme, die eine *„Backdoor“* zum infizierten Rechner öffneten, gewannen immer mehr an Bedeutung. Mit Anbruch des kommenden Jahres waren immer mehr Schadprogramme in der Lage, Schutzmaßnahmen wie Anti-Viren-Software und Personal Firewalls zu deaktivieren, und konnten somit nicht nur ungehindert agieren, sondern lieferten den Rechner weiteren Angriffen schutzlos aus.

Auch rückte das Konzept des *„Social Engineering“,* also die soziale Manipulation des Opfers mit verschiedenen Tricks, seit dieser Zeit immer mehr ins Blickfeld der Malware-Autoren, so gab sich der E-Mail-Wurm *Swen* als Patch von Microsoft aus und wurde von vielen arglosen Benutzern installiert. Der Erfolg bei einem solchen Manipulationsversuch hängt von mehreren Faktoren ab, so muss zunächst das Misstrauen des Opfers zerstreut werden, damit es in dem zu öffnenden Dateianhang keine Bedrohung für seinen Computer sieht, beispielsweise durch die bereits erwähnte Fälschung der Absenderadresse. Als weiterer Erfolgsfaktor ist maßgeblich, dass der Anwender einen Grund hat, die angehängte Datei zu öffnen, sei es durch geweckte Neugier auf ein sehenswertes Foto, oder durch die Schockwirkung, wenn beispielsweise die Mail angeblich vom Bundeskriminalamt (BKA) kommt und den Empfänger über ein gegen ihn eingeleitetes Ermittlungsverfahren informieren soll. Teilweise wurden in den folgenden Jahren Zweifel aber auch dadurch zerstreut, dass mit der Gebühreneinzugszentrale (GEZ) ein vermeintlich vertrauenswürdiger Absender vorlag oder es in der E-Mail augenscheinlich um Tickets für die Fußball-WM 2006 ging. Einige Würmer machen sich für ihre Distribution auch das sogenannte *„Filesharing“* zunutze, indem sie sich unter vielversprechenden Dateinamen als angebliche Film- bzw. Musik-Datei oder Software zum Download zur Verfügung stellen, um dann vom Opfer selbst heruntergeladen und aktiviert zu werden.

Bis Anfang des Jahrtausends sollten einige Schadprogramme durchaus noch die Aufmerksamkeit auf sich ziehen, doch die Entwicklungen ab dem Jahr 2003 zeigten, dass Malware-Autoren die Möglichkeiten erkannt haben, die infizierte Rechner bieten können, so dass sich eine Verschiebung der Interessen abzeichnete. Während das Löschen von Daten (fast) völlig an Bedeutung verlor, wurden die infizierten Rechner neuerdings genutzt, um verteilte DoS-Attacken zu starten, wie zum Beispiel nach der Infizierung durch den *Blaster*-Wurm auf die Update-Webseiten von Microsoft.

Schadprogramme bieten ihren Autoren heutzutage oft die Möglichkeit, sich über eine Backdoor unbefugt Zugriff auf den befallenen Rechner zu verschaffen, indem sie die Mechanismen der Zugangssicherung auf dem betroffenen Computer umgehen. Auf diese Weise können Malware-Programmierer oder ihre Komplizen auf den infizierten Maschinen Daten lesen (und löschen), vor Allem aber können sie Programme ausführen. Dadurch stehen die Rechner als sogenannte *„Bots“,* also als (ferngesteuerte) Roboter, welche neben der Arbeit ihres eigentlichen Benutzers auch die Befehle des Malware-Autors ausführen, für beinahe beliebige Aufgaben zur Verfügung. Weitere gängige Begriffe für Computer, die über einen Backdoor-Zugang gesteuert werden, sind *„Zombies“,* also seelen- bzw. willenlose Untote, welche die Befehle ihres „Meisters“ ausführen, und *„Drohnen“,* also unbemannte und damit ferngesteuerte „Fahrzeuge“ bzw. technische Geräte.

Diese Bots werden üblicherweise in Botnetzen zusammengefasst, die dann über einen sogenannten *„Command and Control*-Server“ zentral gesteuert werden können. Die beiden häufigsten Einsatzgebiete für Botnetze sind großangelegte DDoS-Angriffe, für die aufgrund der großen Anzahl koordiniert steuerbarer Rechner eine große Bandbreite zur Verfügung steht, und der Versand von Spam-Mails. Die Größenordnungen, die ein solches Botnetz erreichen kann, reichen gemäß heise online (2007) im Fall des „Sturm-Wurm-Botnetzes“ bis über 1,7 Mio. infizierte Rechner. Aus diesem Grund stellt ein auch weitaus kleineres Botnetz durchaus eine erhebliche Bedrohung dar, wenn von ihm eine *Denial of Service*-Attacke ausgeht.

In Verbindung mit dem Versand von Massen-Mails spielen diese Botnetze eine zunehmend größere Rolle, deswegen wird dieses Thema im Anschluss an den Überblick über Spam bei der Analyse der Zusammenhänge zwischen Schadprogrammen und unerwünschten E-Mails in Abschnitt 2.1.3 erörtert.

2.1.2 Unerwünschte E-Mails (Spam)

Spam ist ein Phänomen, mit dem früher oder später jeder Internet-Nutzer konfrontiert wird, auch wenn er nicht zwangsläufig selbst „Opfer“ desselben werden muss. Im Englischen werden Spam-Mails auch häufig als *„junk mails“* bezeichnet, was so viel bedeutet wie Ramsch oder Schrott, aber auch Ausschuss. Eine einheitliche Definition ist aufgrund der Tatsache, dass es sich bei Spam um unerwünschte Nachrichten und damit um eine subjektiv wahrgenommene Störung handelt, nur schwer zu treffen. Somit können Spam-Mails nicht an Inhalten festgemacht werden, sondern lediglich an der Eigenschaft, dass sie vom Benutzer nicht erwünscht sind.

Als *„SPAM“* wurde ursprünglich Dosenfleisch der US-amerikanischen Hormel Foods Corporation bezeichnet und stand als Abkürzung für ***sp****iced h****am***[8], also gewürzten Vorderschinken. Im Zweiten Weltkriegs war das 1937 auf den Markt gebrachte Fleisch während der Rationierung in den Vereinigten Staaten von Amerika ein sehr einfach zu bekommendes Nahrungsmittel, dessen die Bevölkerung aber mit der Zeit überdrüssig wurde, so dass die Redewendung „. . . so unnötig wie Büchsenfleisch“ (Spam) entstand.

Dieses Sprichwort wurde in einem Sketch der Comedyserie *„Monty Python's Flying Circus“* aufgegriffen, als in einem englischen Café zu (nahezu) jedem Gericht Spam serviert wurde, teilweise war Spam sogar mehrfach hintereinander in der Menübeschreibung enthalten. Darüber hinaus übertönte eine Gruppe von Wikingern durch ihren Spam-Gesang jegliche Kommunikation, alles in Allem fällt das Wort Spam in den dreieinhalb Minuten über 100 Mal. Dieser Sketch der englischen Komikergruppe *„Monty Python“* wird im Allgemeinen als der Grund dafür gesehen, dass unerwünschte E-Mails heute als Spam bezeichnet werden. Denn während man im Green Midget Café in Bromley zu jedem Essen Spam bekam und durch die Spam-Gesänge sein eigenes Wort nicht mehr verstehen konnte, erhält man Spam-Mails auch ungefragt und in unüberschaubaren Mengen.

Der Begriff Spam ist ein Oberbegriff für verschiedene Arten unerwünschter E-Mails, die, wie hier gezeigt wird, keine disjunkten Mengen sind.

[8] Häufig wird der Name auch auf *„**s**houlder of **p**ork and h**am**“*, *„**s**piced **p**ork **a**nd ha**m**“* oder *„**s**piced **p**ork **a**nd **m**eat“* zurückgeführt.

An erster Stelle sind die *„Unsolicited Bulk E-Mail(s)“ (UBE)* zu nennen, zu Deutsch „unverlangte Massen-E-Mails“, bei welchen es sich ohne näheren Bezug auf den Inhalt um E-Mails handelt, die unaufgefordert in großen Mengen verschickt werden. Diese E-Mails machen den größten Teil der Spams sowie des gesamten E-Mail-Aufkommens aus, da sie die Menge der Werbe-Mails beinahe vollständig einschließen. Neben werbenden Inhalten zählen in diese Kategorie religiöse und politische E-Mails, die teilweise auch missionierenden bis hin zu volksverhetzenden Charakter haben können, auch Spaß-Mails *(Hoaxes)* und Kettenbriefe gehören zu den Massen-Mails. Theoretisch könnten auch massenhaft versendete E-Mails mit betrügerischen Inhalten, wie beispielsweise E-Mails der *„Nigeria-Connection“* oder sogenannte *„Phishing-Mails“,* in diese Kategorie aufgenommen werden.

Bei den *„Unsolicited Commercial E-Mail(s)“ (UCE),* also „unerwünschten Werbe-E-Mails“, handelt es sich um E-Mails mit werbenden Inhalten, die per Definition auch gezielt an potentiell Interessierte verschickt worden sein können und kein Massenphänomen sein müssen. So zählt das unaufgeforderte Versenden eines werbenden Newsletters an Kunden als *UCE,* ohne dass die mengenmäßige Anforderung der Massen-E-Mails erfüllt werden muss. Häufig werden jedoch diese Werbe-Mails in Massen an alle verschickt, die sich durch den Besitz einer E-Mail-Adresse ungewollt zu potentiellen Interessenten gemacht haben, so dass *UBE* und *UCE* eine große Schnittmenge haben. In den massenhaft versendeten Werbe-Mails werden alle vorstellbaren Produkte und Dienstleistungen beworben, seien es Finanzdienstleistungen wie Kredite oder Wertpapiere, medizinische Angebote wie Penisvergrößerungen, lebensverlängernde Maßnahmen oder schlichtweg Medikamente, (teilweise gefälschte) Markenprodukte und Software zu günstigen Preisen, und vieles mehr.

Als dritte große Gruppe unerwünschter E-Mails sind die *„Collateral Spam-Mail(s)“* zu nennen. Als kollaterale Spams werden E-Mails bezeichnet, die aus technischen Gründen verschickt werden und nicht ihres Inhalts wegen, beispielsweise wenn durch eine eingegangene E-Mail eine (automatische) Antwort generiert wird, welche zumeist einem unbeteiligten Dritten zugeschickt wird. Der häufigste Grund für die Entstehung solcher Nachrichten sind mit gefälschtem Absender verschickte Spam-Mails oder von Malware zur Reproduktion erstellte Mails, deren Antworten oder Rücksendungen dann im

Postfach des vermeintlichen Absenders landen, sofern sie überhaupt zugestellt werden können. Dabei werden nicht nur diese sogenannten *„Misdirected Bounces“* in Form von Abwesenheits- oder Unzustellbarkeits-Meldungen als kollateral angesehen, sondern auch vom Empfänger manuell verschickte Reaktionen auf Spam oder Malware-Mails.

Eine von der Firma Ironport (2006) auf dem *„4th German Anti-Spam Summit“* in Köln vorgestellte Statistik besagte, dass 76 % des von ihnen beobachteten Mail-Aufkommens Spam-Mails waren, die sich aus 67 % herkömmlicherweise als Spam bezeichneten Werbe-Mails und 9 % *Misdirected Bounces* zusammensetzten. Lediglich bei 20 % der E-Mails handelte es sich um erwünschte E-Mails, die hier von Ironport „legitime E-Mails“ genannt wurden und oft als *„Ham“* bezeichnet werden, beispielsweise im Zusammenhang mit dem Filter-Programm *SpamAssassin.* In dieser Statistik nicht als Spam eingeordnet waren die Phishing-Mails, die mehr als ein Prozent des Gesamtaufkommens ausmachten, dazu kamen außerdem noch drei Prozent mit Malware verseuchte Mails.

Neben unerwünschten Nachrichten per E-Mail oder per Fax gibt es in den letzten Jahren auch vermehrt Werbung über andere Kommunikationsmedien.[9] Darüber hinaus gibt es auch Spam für Mobiltelefone,[10] wobei es sich sowohl um unerwünschte SMS-Nachrichten als auch um Anrufe handelt, die teilweise nur den Zweck verfolgen, den Angerufenen zum Rückruf zu bewegen. Diese Anrufe führen dann oft zu teuren Mehrwertdiensten und verursachen dadurch für das Opfer hohe Kosten.

Gering sind dagegen die Kosten für das Versenden von Spam-Mails, weswegen sich diese Strategie für den Versand von Werbung überhaupt lohnt, dabei muss sich das Geschäftsmodell der Spammer nicht auf den Versand der eigenen Werbe-Mails beschränken. So boten laut novirdata (2005) Spam-Versender bereits vor Jahren an, zu günstigen Preisen Werbung für fremde Produkte zu machen, damals konnte der Versand von 40 Mio. E-Mails für $ 250 in Auftrag gegeben werden. Auch lässt sich mit dem Verkauf von E-

[9] Unerwünschte Werbeanrufe per Internet-Telefonie, auch als *Voice over IP* bekannt, werden als SPIT *(„**Sp**am over **I**nternet **T**elephony“)* bezeichnet, Werbung über Instant Messenger wie ICQ oder IRC als SPIM *(„**Sp**am over **I**nstant **M**essaging“).*

[10] Werbung über Mobiltelefone wird SPOM *(„**Sp**am **o**ver **M**obile Phone“)* genannt.

Mail-Adressen Geld verdienen, so konnten gemäß Microsoft (2005) in Deutschland 750 Mio. Adressen für $ 499 erstanden werden.

Wenn für den fremdvergebenen Versand von 40 Mio. Werbe-Mails jedoch nur $ 250 bezahlt werden müssen, dann belaufen sich die Kosten für 1.000 E-Mails auf gut einen halben US-Cent.[11] Aus diesem Grund können gemäß Vircom (2004) schon bei einer Kaufquote von 0,0001 % Gewinne erwirtschaftet werden, das heißt, dass selbst, wenn nur jeder Millionste Empfänger das beworbene Produkt kauft, die Werbeaktion per Spam ein (finanzieller) Erfolg ist.

Der Hauptteil der Kosten geht bei Spam-Mails somit zu Lasten der Empfänger, die als Privatpersonen bei vielen Anbietern für E-Mail-Dienste aufgrund des eingeschränkten Speichervolumens regelmäßig die unerwünschten Nachrichten löschen oder für mehr Speicherplatz bezahlen müssen. Ansonsten laufen sie Gefahr, dass ihr Postfach mit Spams bis zur Grenze des zugestandenen Speichervolumens „vollläuft“ und ankommende E-Mails abgelehnt werden, oder dass gemäß Sipior et al. (2004) ihr Zugang vom Provider, also dem Anbieter des Mail-Dienstes, gesperrt wird.

Unternehmen müssen, sofern sie ihren Mail-Server selbst betreiben, als eine Folge der Spam-Flut zumindest zusätzliche Hardware für die Erweiterung des Speicherplatzes anschaffen oder richten sich bevorzugt einen Spam-Filter ein, um auch den Verlust an Arbeitszeit auf Seiten der Mitarbeiter durch das manuelle Aussortieren der unerwünschten Mails gering zu halten.

Obwohl der Großteil des aktuellen E-Mail-Aufkommens aus Spam-Mails der verschiedenen Kategorien besteht, ist es auch heute noch möglich, ein elektronisches Postfach zu verwenden, welches nicht von der Spam-Flut erreicht wird. Wichtiger als die verschiedenen Filtermaßnahmen zum Erkennen und Entfernen unerwünschter E-Mails ist ein verantwortungsbewusster Umgang mit der eigenen E-Mail-Adresse. So führt gemäß Clement et al. (2008) die Weitergabe der eigenen E-Mail-Adresse an Unbekannte zu signifikant höheren Arbeitszeitverlusten durch das Aussortieren bzw. Löschen von Spam-Mails.

[11] Auf Basis des mittleren Sortenkurses von 2005 lagen damit die Kosten für 1.000 Spam-Mails unter einem halben Eurocent, zum Vergleich kostet in Deutschland jedoch allein der Vertrieb von (Papier-)Prospekten mehr als einen Eurocent pro Stück.

Eine Studie der *Federal Trade Commission (FTC)*[12] (2005) hat ergeben, dass 100 % aller E-Mail-Adressen, die in einem *Chatroom* genannt wurden, danach Spam erhielten, dabei lag der Rekord bei acht Minuten zwischen der Bekanntgabe der Adresse und dem Erhalt der ersten Spam-Mail. E-Mail-Adressen, welche im Rahmen dieser Studie in einer *Newsgroup* oder auf einer Webseite veröffentlicht wurden, erhielten demnach infolge der Publikmachung in 68 % der Fälle unerwünschte Werbe-Mails.

Ist eine E-Mail-Adresse erst einmal in einer Datenbank von Spammern eingetragen, so ist es nicht mehr möglich, diese Adresse dort wieder entfernen zu lassen. Zwar wird teilweise in Spam-Mails die Möglichkeit gegeben, einen Link anzuklicken, um die Mail-Adresse (angeblich) aus der Liste austragen zu lassen, diese Links sind jedoch laut Steve Wernikoff von der FTC meistens tot.[13] Er widersprach damit auch der langjährigen Annahme, das Anklicken dieser Links führe nur dazu, durch die Bestätigung einer Aktivität der Adresse noch mehr Spam-Mails zu bekommen. Vielmehr lohne es sich gemäß Wernikoff für die Spammer nicht, die Adressen in den Datenbanken zu validieren, weil die Kosten für die Überprüfung einer Adresse jene für das Versenden an nicht genutzte Adressen erheblich überstiegen.

Um eine E-Mail-Adresse, die regelmäßig unerwünschte E-Mails erhält, weiterhin vernünftig nutzen zu können, ohne sich selbst permanent mit den Werbe-Mails beschäftigen zu müssen, empfiehlt sich die Einrichtung eines (automatischen) Filter-Programms. Für diese Filter-Mechanismen gibt es zahlreiche Konzepte, die teilweise entwickelt wurden, um zumindest vorübergehend der Spam-Flut Herr zu werden. Doch wie bei der Entwicklung von Schutzmaßnahmen gegen Schadprogramme und neuen Ideen, diese zu umgehen oder auszuschalten, handelt es sich auch hier um einen Wettlauf zwischen „Hase und Igel“, also Filter-Entwicklern und Spam-Autoren, bei welchem der Erfolg der Filter nur kurz anhält.

In der Anfangszeit der Spam-Mails wurde die elektronische Werbung mit einer regulären Absender-Adresse von speziellen Spam-Servern verschickt,

[12] Die *Federal Trade Commission* ist eine US-amerikanische Bundesbehörde und neben der Wettbewerbskontrolle auch für den Verbraucherschutz zuständig.

[13] Steve Wernikoff sprach in diesem Zusammenhang auf dem *„3rd German Anti-Spam Summit“* von der *„vast majority“* (zit.).

und die Werbebotschaften waren als klar lesbarer Text enthalten. Dies führte einerseits zu der Entwicklung sogenannter *„Blacklists“* und *„Whitelists“*, andererseits konnten auch einfache *„Contentfilter“* eingesetzt werden.

Diese Schwarzen bzw. Weißen Listen[14] enthalten Informationen über Absender-Adressen, -Domänen oder -IPs, welche als Spammer bekannt und unerwünscht sind bzw. als vertrauenswürdig eingestuft und erwünscht sind. Auf diese Weise können die E-Mails anhand der Absenderinformationen gefiltert werden, ohne sich näher mit dem Inhalt zu beschäftigen. Unter Zuhilfenahme eines Inhaltsfilter lassen sich bestimmte Begriffe wie „Viagra“ oder *„replica“* als unerwünscht einstufen, bei Ökonomen könnte hingegen „Stock“ trotz einer steigenden Zahl Börsen-bezogener Spam-Mails als erwünscht kategorisiert werden. Dabei ist eine gewissenhafte Auswahl der zu filternden Buchstabenfolgen wichtig, da beispielsweise das Ausfiltern des Wort(teil)es „sex“ auch das „Zufallsexperiment“ betrifft. Spam-Filter wie der *SpamAssassin* bewerten bestimmte Eigenschaften und Inhalte von E-Mails mit einem bei der Konfiguration angegebenen Gewicht und summieren die einzelnen Ergebnisse zu einem Gesamtwert, überschreitet dieser einen (veränderbaren) Grenzwert, so wird die Nachricht als Spam eingestuft. In Verbindung mit Schwarzen und Weißen Listen können empfangene E-Mails vor der inhaltlichen Filterung auf Einträge in den Listen überprüft werden, so dass nur diejenigen Nachrichten näher analysiert werden müssen, die nicht aufgrund dieser Listen bereits abgelehnt oder angenommen wurden.

Im Zusammenhang mit dem Ausfiltern von E-Mails durch den Betreiber eines Mail-Servers ist in Deutschland zu beachten, dass das Löschen von E-Mails nur mit ausdrücklicher Zustimmung des Empfängers geschehen darf, da das unberechtigte Unterdrücken elektronischer Nachrichten einen Verstoß gegen das Post- und Fernmeldegeheimnis darstellt.[15]

[14] Solche Listen können lokal gepflegt werden, *Blacklists* werden aber auch im Internet von verschiedenen Anbietern zur Verfügung gestellt.

[15] Nach § 206 Abs. 2 Nr. 2 StGB „wird bestraft, wer als Inhaber oder Beschäftigter eines [...] Unternehmens [, das geschäftsmäßig Post- oder Telekommunikationsdienste erbringt,] unbefugt [...] eine einem solchen Unternehmen zur Übermittlung anvertraute Sendung unterdrückt“. Die Zustimmung zu einer Filterung von E-Mails kann auch durch das Akzeptieren der Allgemeinen Geschäftsbedingungen (AGB) zu einem Teil des Vertragsabschlusses gemacht werden.

Im Laufe der Jahre wurden diese Schutzmaßnahmen gegen Spam jedoch Stück für Stück umgangen, so dass es inzwischen immer schwieriger geworden ist, Spam-Mails zu identifizieren. Der Überprüfung von Absender-Adressen wirkten Spammer durch gefälschte Absender entgegen, was durch die Überprüfung auf die tatsächliche Existenz dazu geführt hat, dass zunehmend die Adressen unschuldiger Dritter als Absender missbraucht wurden. Diese erhielten dann auch die als unzustellbar zurückgeschickten Antworten.

Auch wurden Werbe-Mails zunehmend nicht mehr von (zentralen) Spam-Servern verschickt, sondern vermehrt von Millionen von Computern, die in Botnetzen ferngesteuert und als Spam-Server missbraucht werden. Diese Entwicklung, auf die in Abschnitt 2.1.3 näher eingegangen wird, führte dazu, dass die herkömmlichen Schwarzen Listen für Spam-Server kaum noch verwendet werden können, vielmehr müssen dynamische Datenbanken die aktuellen Veränderungen in den Botnetzen wiedergeben.

Das Filtern nach bestimmten Wörtern führte zunächst zu leichten Veränderungen wie beispielsweise „Vi@gra“ oder „V1agra“, um Spam-Filter auf der Suche nach „Viagra“ zu täuschen. Auf diese Weise mussten zunehmend komplexere Filterregeln erstellt werden, zwischenzeitlich führte dieses Vorgehen bis hin zur völligen Entstellung des filtergefährdeten Wortes, das beispielsweise als „\/1a 9r@“ auch für Menschen nur noch schwer zu entziffern war.

Im Jahr 2004 gingen laut eleven (2007) die Spammer vermehrt dazu über, ihre Werbebotschaft in Bildern zu verschicken, dabei wurden zunächst nur Grafikdateien verschickt. Als jedoch die Spam-Filter E-Mails mit Bild und ohne Text verstärkt als typische Spam-Eigenschaft einzustufen begannen, wurden die Bilder durch Text ohne Zusammenhang zur eigentlichen Werbebotschaft ergänzt. So führte das Anhängen von Auszügen aus literarischen Werken wie dem Fantasy-Epos *„The Lord of the Rings“* dazu, dass die E-Mails sinnvoll ausformulierte Sätze ohne werbetypische Inhalte enthielten und vorübergehend als erwünschte E-Mails akzeptiert wurden. Durch das Anlegen von Grafik-Datenbanken konnten die als *„Image Spam“* bekannten werbenden Bilder jedoch mit der Zeit ebenfalls identifiziert werden.

Ende des Jahre 2005 begannen Spammer gemäß eleven (2007), ihre Bilder mit zufälligen kleinen Veränderungen zu versehen, die zwar vom menschlichen Auge wahrgenommen werden, von ihm aber durch die unbeeinträchtigte Lesbarkeit nicht als störend empfunden werden. Für Spam-Filter stellt die

„Wiedererkennung“ solcher Bilder, die unter dem Begriff *„Randomized Image Spam“* zusammengefasst werden, jedoch ein erhebliches Problem dar. Als Möglichkeiten für die Manipulation der Bilder seien beispielsweise die Veränderung von Farben, Schriftposition oder Schriftart zu nennen, welche bei der Betrachtung durch den Menschen keine Auswirkungen haben, die Bitfolgen in der vom Computer gelesenen Bilddatei hingegen deutlich beeinflussen. Auch das zufällige Einfügen kleiner Punkte, von Ironport (2006) als *„Polka Dots“* bezeichnet, stört lediglich Computer – und eventuell Ästheten.

Ein vom Menschen bei korrekter Darstellung auf dem Bildschirm nicht erkennbarer Trick ist dagegen das Zusammensetzen eines Werbebildes aus verschiedenen kleineren Bildern, das je nach Quelle beispielsweise *„Sliced Image“* [El07] oder *„Slice & Dice“*[16] [I06] genannt wird. Dabei wird ein Bild in zufällige Rechtecke unterteilt, welche der Spam-Mail dann als einzelne Bilder angehängt werden und durch die Einbettung in *HTML*-Code vom Mail-Browser dergestalt zusammengefügt werden, dass auf dem Bildschirm nur ein einzelnes (Gesamt-)Bild zu erkennen ist. Auf diese Weise sollte das Anlegen von Bilder-Datenbanken erschwert werden, da auch hier immer neue Grafiken aufgenommen werden müssen. Da das Datenvolumen für mehrere kleine Bilder gegenüber jenem eines vergleichbar großen einzelnen Bildes steigt, erreichte die Größe einer durchschnittlichen Spam-Mail gemäß eleven (2007) im April 2006 ihren Höhepunkt. Auf diese Weise wuchs in jener Zeit das Spam-Volumen gegenüber den Vormonaten nicht nur durch die Anzahl an Werbe-Mails, sondern auch durch die Tatsache, dass die Spam-Mails im Frühjahr 2006 ungefähr zehnmal so groß waren wie im Vorjahr.

Aktuell hat sich zumindest eine der geschilderten Methoden zur Umgehung von Filtermechanismen wieder umgekehrt, da in der Zwischenzeit wieder viele Spam-Mails mit im Klartext lesbaren Schlagworten wie *„drugs“* oder dem berühmten „Viagra“ im Umlauf sind. Unverändert bleibt jedoch der Anstieg des Spam-Volumens, welches in einem Zeitraum von zwei Jahren laut eleven (2007) um mehr als 3.500 % gestiegen ist.[17]

Bei der Verwendung von Filtermaßnahmen dürfen jedoch die sogenannten *„False Positives“* oder „Falschen Positiven“ nicht außer Acht gelassen werden,

[16] Die Vorgehensweise lässt sich am Besten mit „Zerschneiden und Zusammenwürfeln“ (oder „Zusammensetzen“) übersetzen.

[17] Als Beispiel diente ein Blue Chip-Unternehmen im Zeitraum 24.08.2005 bis 23.08.2007.

bei denen es sich analog zum Testen von Hypothesen um einen Fehler 1. Art oder α-Fehler handelt. Bei der Filterung von E-Mails lautet die Nullhypothese H_0, dass es sich bei einer E-Mail nicht um Spam handelt, führt jedoch die Überprüfung ihrer Eigenschaften fälschlicherweise zu einer Klassifikation als Spam-Mail, so wird sie unberechtigterweise gekennzeichnet oder sogar gelöscht. Dieser Effekt ist natürlich nicht erwünscht, vielmehr sollte das Hauptaugenmerk bei der Filterung von E-Mails mehr auf einem geringen Anteil an *False Positives* liegen als auf einem möglichst geringen Anteil von Spam-Mails, die nicht als solche eingestuft werden. So sprach R. Wienholtz von CTO STRATO (2007) von einem Fokus auf „Ham“ bei der Filtereffizienz und schlussfolgerte, dass ein Blocken aller E-Mails eine Spam-Filterung von 100 % erreiche.

2.1.3 Zusammenhang zwischen Malware und Spam

Lange Zeit wurden Malware und Spam als getrennte Phänomene betrachtet, da Schadprogramme seit jeher als Bedrohung wahrgenommen werden, während unerwünschte (Werbe-)Mails, vergleichbar mit gedruckten Werbeprospekten im Briefkasten, bis vor wenigen Jahren von vielen nur als Belästigung angesehen wurden. Im Jahr 2003 überstieg der Anteil der Spam-Mails am Gesamtaufkommen erstmals den Anteil der erwünschten Mails, mit schon damals stark steigender Tendenz. Inzwischen geht die *European Network and Information Security Agency (ENISA)* (2007) von über 93 %[18] Anteil der unerwünschten E-Mails aus, so dass die Quote der „Ham-Mails“ fast schon verschwindend klein ausfällt.

Bereits im Jahr 2005 sprach ein Vertreter der FTC davon, dass mehr als die Hälfte aller Spam-Mails von Botnetzen versendet werde, diese Meinung wurde von mehreren Quellen bestätigt. Die *Messaging Anti Abuse Working Group (MAAWG)* (2005) vermutete damals sogar schon eine Quote von mehr als 80 %, eine aktuelle Studie der FTC (2007) hat nun ergeben, dass Botnetze inzwischen für 95 % aller Spam-Mails verantwortlich sind.

[18] Eine Untersuchung bei E-Mail-Providern ergab, dass ungefähr 88 % der Mails als Spam abgelehnt wurden, vom Rest aber immer noch über 45 % als Spam identifiziert wurden. Der Anteil erwünschter E-Mails kann demnach höchstens bei 55 % gelegen haben, am Gesamtaufkommen gemessen entspräche das 6,6 %.

Ein konkretes Beispiel für die Verknüpfung von Malware und Spam über Botnetze gab Frank Eißmann vom Landeskriminalamt Baden-Württemberg am Fall des aus dem Schwarzwald stammenden Malware-Autors „AGO“. Die Exemplare des nach ihm benannten Wurms *Agobot* nutzten verschiedene Sicherheitslücken von Windows-Systemen aus und verbreiteten sich über die Infrastruktur anderer Schadprogramme. Die Verbreitung wurde *Agobot* auch dadurch erleichtert, dass der Wurm *Sasser* auf dem PC eine Tabelle der von ihm infizierten Rechner hinterließ, welche sich der neue Eindringling zunutze machte. Für 30.000 Euro pro Monat konnte nun eines der Botnetze angemietet werden, sowohl zum Versand von Spam-Mails als auch für DDoS-Angriffe, das CERT Stuttgart sprach in diesem Zusammenhang von 140.000 Bots in einem Netz.

Botnetze weisen eine erstaunliche Dynamik auf, denn während einzelne Rechner nach der Entdeckung und Entfernung des Schadprogramms aus dem Netz verschwinden, wächst die Anzahl der Zombies weiter, so dass während der Desinfektion eines Rechners offensichtlich zeitgleich mehrere neue Rechner befallen werden. So wurden laut Spamhaus (2007) an einem „normalen“ Tag von der eigenen *„Exploits Block List“ (XBL)* fast 900.000 neue eindeutige IP-Adressen von Bots identifiziert.[19] Auch ist die Geschwindigkeit verblüffend, mit welcher die neu in einem Netz aufgenommenen Bots ihre Arbeit beginnen, so entdeckte Spamhaus (2007), dass zwischen der Infektion mit dem Wurm *Warezov* und dem Versand der ersten Spam-Mail nur 36 Sekunden vergehen.

Inzwischen sind also Malware und Spam sehr eng miteinander verknüpft, da die Verbreitung bestimmter Schadprogramme stark ursächlich für die Veränderung des Spam-Aufkommens ist. Dennoch muss das Schadenspotential der beiden Internet-Phänomene klar voneinander abgegrenzt werden, eine Spam-Mail mit einer Malware-verseuchten E-Mail zu vergleichen, entspräche dem Vergleich einer Postwurfsendung mit einer Briefbombe. Während Postwurfsendungen als Belästigung angesehen werden können und auch in elektronischer Form bei entsprechend großen Mengen den Briefkasten verstopfen können, geht von „elektronischen Briefbomben“ auch ein tatsächliches Gefahrenpotential aus.

[19] Eine Messung am 24.06.2007 ergab 882.565 neue IP-Adressen in der Bot-Datenbank.

Während manuelle Angriffe durch Hacker oder gezielte DDoS-Attacken im Normalfall nur Unternehmen treffen, stellen Schadprogramme eine Gefahr für alle dar, deren Computer ans Internet angeschlossen sind. Durch die zunehmende Zahl von Computern, die in Botnetzen nicht nur den Befehlen ihrer Besitzer, sondern auch ihrer „Besetzer“ in Form von Botnetz-Betreibern gehorchen, wird die IT-Sicherheit aller Internet-Nutzer akut bedroht. Diese Sicherheit zu gewährleisten kostet sehr viel Geld, doch ihre Sicherstellung dürfte vermutlich immer noch erheblich günstiger sein als ihre Wiederherstellung. Aber wie hoch sind diese Kosten für IT-Sicherheit, was kostet der (erfolgreiche) Schutz vor den Bedrohungen aus dem Internet, und wie teuer kommt ein Opfer beispielsweise ein Vorfall durch Malware zu stehen? Wie sollen Kosten gemessen werden, die durch Investitionen in Präventionsmaßnahmen vermieden werden? Welche Kosten entstehen bei der erfolgreichen Abwehr der Spam-Flut durch die Einrichtung von Spam-Filtern, und welche entstehen durch die Werbe-Mails, welche durch den Filter oder gar ungehindert beim Empfänger ankommen? Den Problemen bei der Bewertung dieser Kosten widmen sich die folgenden Abschnitte.

2.2 Stand der Forschung

In der Wissenschaft wurden die Phänomene Malware und Spam in den vergangenen Jahren hauptsächlich aus technischer und juristischer Sicht betrachtet. Es gibt zahlreiche Veröffentlichungen zu technischen Lösungen für die beiden Probleme, beispielsweise zu Erkennungs- und Filteralgorithmen. Doch einige dieser technischen Maßnahmen sind in der Zwischenzeit nur noch eingeschränkt nutzbar, so war früher das Blocken von IP-Adressen, welche als Spam-Versender identifiziert worden waren, ein erfolgversprechender Ansatz zur Reduzierung der Spam-Flut.

In der Zwischenzeit werden Spam-Mails jedoch wie im vorherigen Abschnitt beschrieben nicht mehr hauptsächlich von (identifizierbaren) Spam-Servern verschickt, sondern zunehmend über Botnetze und somit von den Computern unbedarfter Benutzer. Da die Zahl dieser infizierten Rechner täglich steigt und immer wieder einzelne Maschinen nach der Entdeckung und Entfernung des Schadprogramms aus den Botnetzen verschwinden, ist

eine vollständige und aktuelle Erfassung dieser dynamischen Spam-Server-Landschaft nur noch schwer möglich. Auch bei den Filtermechanismen lassen sich die Spam-Versender immer neue Möglichkeiten einfallen, um zumindest kurz- bis mittelfristig die Mechanismen zur Erkennung von Spam-Mails auszuhebeln und damit den Schutz vor unerwünschten E-Mails zu umgehen.

Aus diesen Gründen wird von Experten eine grundlegende Veränderung der E-Mail-Kommunikation diskutiert, wie beispielsweise eine zahlenmäßige Einschränkung der E-Mails, die täglich von einem E-Mail-Konto verschickt werden können.

Rechtliche Maßnahmen zur Bekämpfung oder Eindämmung der Spam- und Malware-Problematik werden in der Literatur ebenfalls diskutiert, hier findet man die größte Hürde für Lösungen in der Internationalität des Internets. Die Gesetze eines Landes greifen im Normalfall nur innerhalb der eigenen Grenzen, so dass juristische Schritte gegen die Spam-Flut nur einen kurzfristigen Erfolg bringen können, bis die Spammer gemäß L. Zhang (2005) ins Ausland ausgewichen sind.

So wurde das Gesetz gegen den unlauteren Wettbewerb (UWG) zwar im Jahr 2004 umfassend novelliert, um Verbraucher *de jure* mit § 7 UWG neben unaufgeforderter Telefonwerbung auch vor unerwünschten E-Mails und damit vor „Unzumutbare[n] Belästigungen“ zu schützen. *De facto* greift dieses Gesetz jedoch nur bei unerwünschter Werbung aus dem Inland, da Spam-Versender im Ausland üblicherweise nicht von deutschen Strafverfolgungsbehörden belangt werden können. Darüber hinaus werden eigentlich weniger die Verbraucher, sondern vielmehr die Mitbewerber geschützt, da nur diesen neben Verbraucherverbänden sowie Industrie- und Handelskammern die Möglichkeit eingeräumt wird, gegen Spam-Versender zu klagen.

Der Entwurf eines Anti-Spam-Gesetzes zur Erweiterung des Teledienstegesetzes (TDG) um Vorgaben für den Versand von Werbe-Mails wurde zwar im Deutschen Bundestag am 17. Februar 2005 in erster Lesung beraten, jedoch nicht mehr in der 15. Legislaturperiode verabschiedet. Dabei ging es nicht um das Verbot von unerwünschten Werbe-Mails im Allgemeinen, sondern um die nicht zulässige Verschleierung des kommerziellen Inhalts und des Absenders der E-Mail. Diese Regelung floss in § 6 Abs. 2 des Telemediengesetzes (TMG) ein, welches am 1. März 2007 in Kraft getreten ist:

„Werden kommerzielle Kommunikationen per elektronischer Post versandt, darf in der Kopf- und Betreffzeile weder der Absender noch der kommerzielle Charakter der Nachricht verschleiert oder verheimlicht werden. Ein Verschleiern oder Verheimlichen liegt dann vor, wenn die Kopf- und Betreffzeile absichtlich so gestaltet sind, dass der Empfänger vor Einsichtnahme in den Inhalt der Kommunikation keine oder irreführende Informationen über die tatsächliche Identität des Absenders oder den kommerziellen Charakter der Nachricht erhält.“

Ein Verstoß gegen dieses Verbot wird bislang jedoch nur als Ordnungswidrigkeit behandelt und mit einem Bußgeld geahndet. Über eine strafrechtliche Verfolgung der Versender von Spam wird in letzter Zeit ebenfalls debattiert, wie beispielsweise die Dissertation von T. Frank (2004) zeigt. Auch wird in der Literatur die Haftungsfrage für das (unbewusste) Verbreiten von Schadprogrammen diskutiert, während einige Autoren unter bestimmten Voraussetzungen eine Haftungsverpflichtung für Unternehmen sehen, wird diese für Privatpersonen überwiegend verneint.[20]

Vor vergleichbaren Problemen steht der US-amerikanische *„CAN-SPAM Act of 2003“*[21], der ebenfalls nur Richtlinien für das Versenden von Werbe-Mails vorgibt, ohne den Versand unerwünschter E-Mails tatsächlich zu unterbinden. Aus diesem Grund wird das Gesetz von Kritikern auch als *„YOU-CAN-SPAM Act“* bezeichnet, da es *per se* nicht das Versenden von Werbe-Mails ohne Zustimmung des Empfängers verbietet, sondern lediglich Einschränkungen macht wie das Verbot explizit sexueller Inhalte ohne Kennzeichnung in der Betreffzeile. Ähnlich wie in den deutschen Gesetzen muss ein korrekter Absender angegeben werden, zusätzlich eine physikalische, also nicht-virtuelle Adresse des Werbetreibenden. Außerdem muss die E-Mail ein *„Unsubscribe“* enthalten, also dem Empfänger ein Mechanismus zur Verfügung gestellt werden, mit welchem er die Werbesendung abbestellen kann, um zukünftig zumindest von diesem Anbieter keine Werbung mehr zu erhalten.

[20] Unberührt davon ist das *Erstellen und Verbreiten* von Malware als Computersabotage nach § 303 b StGB eine strafbare Handlung.

[21] ***C****ontrolling the* ***A****ssault of* ***N****on-****S****olicited* ***P****ornography* ***A****nd* ***M****arketing Act of 2003 (CAN-SPAM, 15 U.S.C. §§ 7701-7713, 18 U.S.C. § 1037).*

Die ökonomische Betrachtung der in dieser Arbeit thematisierten Gefahren aus dem Internet hat bislang noch wenig Eingang in die Forschung gefunden, dabei gibt es zur Spam-Problematik schon erste Studien. M. Clement et al. (2008) sprechen in ihrer aktuellen Veröffentlichung „Kosten und Kostentreiber von unerwünschten Werbemails (Spam)“ von einer Forschungslücke, welcher man sich mit der vorgelegten empirischen Untersuchung widmen wolle, und auch K. Joseph und A. Thevaranjan (2008) bestätigen, dass es bei der Quantifizierung der Kosten von unerwünschten E-Mails noch erheblichen Forschungsbedarf gibt.

Der Bericht der Kommission der Europäischen Gemeinschaften (2004) fasste in Kürze die wichtigsten Ergebnisse der bis dato veröffentlichten Studien zusammen. So schätzten die Analysten von Ferris Research im Jahr 2003 die durch Spam verursachten Kosten für europäische Unternehmen auf Basis von Produktivitätsverlusten auf 2,5 Mrd. Euro, im selben Jahr bezifferte der Software-Anbieter MessageLabs Ltd. die Spam-Kosten allein für britische Unternehmen auf 4,6 Mrd. Euro[22]. Clement et al. (2008) betonten bezugnehmend auf eine Studie von Nucleus Research (2004), dass sich Management-Studien aber zumeist als wenig fundiert herausstellten. So werde nach Ansicht der Autoren auf Basis weniger, allgemeiner Kennzahlen eine Schätzung der Kosten sowohl für das gesamte Unternehmen als auch für die Mitarbeiter durchgeführt, ohne die individuellen Kosten der einzelnen Mitarbeiter einzubeziehen.

Im Rahmen ökonomischer Betrachtungen des Themas werden zunehmend Regelungsmaßnahmen zur Eindämmung der Spam-Mengen diskutiert, beispielsweise schlugen Joseph und Thevaranjan (2008) die Einführung einer Art Porto für E-Mails vor. Ein weiterer in diesem Aufsatz vorgestellter Ansatz ist ein sogenanntes *„Bonded Sender“* Programm, bei welchem eine zentrale Instanz eine *Whitelist* führt, für deren Mitglieder ein Empfänger erreichbar ist. Erhält die Kontrollinstanz eine Mail von einer nicht gelisteten E-Mail-Adresse, so muss für die Zustellung an den eigentlichen Empfänger ein Geldbetrag hinterlegt werden, welcher nur zurückerstattet wird, wenn die E-Mail vom Empfänger nicht als Spam gemeldet wird. L. Zhang (2005) stellte aber

[22]Der im Juni 2003 errechnete Betrag von £ 3,2 Mrd. wurde auf Basis des damals gültigen Sortenkurses umgerechnet.

fest, dass solche (Markt-)Lösungen noch nicht in größerem Umfang erfolgreich umgesetzt wurden und erwartete in Anbetracht der Internationalität des Problems und der damit verbundenen Abstimmungsschwierigkeiten auch keine baldige Änderung.

2.2.1 Kosten und Kostentreiber von Spam

Eine systematische Analyse der Kosten von unerwünschten Werbe-Mails erfolgte in einer Studie von M. Clement, D. Papies und H. J. Boie (2008), bei welcher an der Christian-Albrechts-Universität zu Kiel eine umfangreiche Erhebung in zwei Befragungswellen durchgeführt wurde. Bei einer Stichprobe von ursprünglich (exakt) 1.000 Universitätsmitarbeitern wurde durch Regressionen das Mittel der jährlichen Kosten je Mitarbeiter auf 531 Euro (2004) bzw. 447 Euro (2005) geschätzt. Diese Werte wurden auf Basis der Arbeitszeitverluste in Verbindung mit den Bruttoarbeitslöhnen errechnet, vorrangigen Einfluss hatte das teilweise tägliche manuelle Aussortieren bzw. die Überprüfung des automatisierten Vorgangs auf *False Positives*. Berücksichtigt wurde aber auch die Suche nach geeigneten Filtermaßnahmen sowie die Installation und Konfiguration der entsprechenden Software.

Unter Verweis auf den Bericht der Kommission der Europäischen Gemeinschaften (2004) fassten Clement et al. (2008) die direkten und indirekten Kosten von Spam zusammen. Demnach entständen direkte Kosten durch Arbeitszeitverluste, wenn durch das Aussortieren der Spam-Mails die Effizienz und Produktivität am Arbeitsplatz beeinträchtigte werde. Auch koste die Planung und Umsetzung entsprechender Schutzmaßnahmen die IT-Abteilungen sowohl Zeit als auch Geld, und es müsse von Seiten der E-Mail-Provider mehr Bandbreite und Speicherkapazität für die Spam-Flut zur Verfügung gestellt werden. Weiterhin würden Kosten durch Rufschädigung oder durch falsche Eintragungen auf *„Blacklists“* verursacht.

Indirekte Kosten träten hingegen auf, wenn bedingt durch Filtermechanismen *False Positives* technisch entfernt oder vom Empfänger nicht gelesen würden, da sie fälschlicherweise als Spam identifiziert wurden. Außerdem würden gemäß des Kommissions-Berichts weitere erhebliche Kosten dadurch entstehen, dass Spam zunehmend zur Verbreitung von Malware genutzt wür-

de. Dieser Behauptung wurde hingegen von Experten auf den *„German Anti-Spam Summit“[s]* wiederholt widersprochen, da eine infizierte Spam-Mail sowohl den Spam-Filter als auch den Virenschutz erfolgreich umgehen müsse, um ihren Empfänger zu erreichen. Daher sei es nicht im Sinne der Versender, die Erfolgschancen einer Werbe-Mail durch ein angehängtes Schadprogramm zu senken. Dennoch können Spam-Mails ebenso wie *„Ham-Mails“* Malware enthalten, so dass diese auch von G. Schryen (2004) erwähnten indirekten Kosten nicht zu vernachlässigen sind.

Die Universität Kiel, an welcher die Studie durchgeführt wurde, entspricht gemäß Clement et al. mit seinen etwa 8.000 Mitarbeitern einem mittelgroßen Unternehmen, von welchen ca. 5.000 zu Beginn der Umfrage im Oktober 2004 direkt per E-Mail erreicht werden konnten. Von den angeschriebenen Universitätsangehörigen füllten mit exakt 1.000 Personen ca. 20 % den Fragebogen vollständig aus, ein Jahr später nahmen von diesen Teilnehmern noch 44 %, also insgesamt 440 an der zweiten Befragungswelle teil. Die Ergebnisse des Panels mit 440 Beobachtungen wurden im Rahmen der Analysen von Clement et al. vorrangig diskutiert und stehen auch in diesem zusammenfassenden Abschnitt im Mittelpunkt, daneben erfolgte in dem Artikel auch die Betrachtung der Resultate für alle 1.000 Teilnehmer.

In der ersten Welle wurden im Mittel fast 45 % der empfangenen E-Mails von den Befragten als Spam wahrgenommen, dieser Anteil verzeichnete in der zweiten Welle einen signifikanten Anstieg auf knapp über 50 % – der Median stieg im gleichen Zeitraum von 40 auf 50 %. Diesbezüglich wurde von den Autoren erwähnt, die hohen Werte seien durchaus plausibel, da Universitäten schon früh an das Internet angeschlossen waren und die Mail-Adressen der Mitarbeiter auf den universitären Webseiten zur Verfügung gestellt wurden. Da der Spam-Anteil im Internet, wie auf Seite 26 beschrieben, schon im Jahr 2003 den Anteil der erwünschten E-Mails überstiegen hatte, lagen die in der Umfrage erhobenen Werte sogar noch unter dem damaligen netzweiten Durchschnitt.

Die im Vorfeld von Clement et al. geführten Expertengespräche ergaben eine vorrangige Betrachtung der Kosten durch Arbeitszeitverluste, da sie in mehreren Fällen als wichtigste Komponente angesehen worden waren.

Die Resultate der Regressionen ergaben, dass in erster Linie das manuelle Aussortieren bzw. das Überprüfen der automatisch vorsortierten Spam-Mails einen täglichen zeitlichen Aufwand erforderte, welcher in der ersten Welle im Mittel bei 4,73 Minuten lag und in der zweiten Welle signifikant auf 4,20 Minuten sank. Hinzu kamen Arbeitszeitverluste für einmalige Maßnahmen wie die Recherche und die Einrichtung von Filtermaßnahmen in Eigenverantwortung oder durch einen technisch versierteren Kollegen. Auf der Basis von 250 Arbeitstagen ergaben sich aus der täglich investierten Arbeitszeit und den einmaligen Vorgängen ein Verlust von gut 1214 Minuten im Jahr 2004 sowie fast 1079 Minuten im Jahr 2005, was einen signifikanten Rückgang bedeutete.

Die Berechnung der jährlichen Kosten für die Universität Kiel auf Mitarbeiterseite führte unter Annahme der Repräsentativität zu einer Summe von 2,235 Mio. Euro für 5.000 Mitarbeiter. Die Aufwendungen des universitären Rechenzentrums von 15.120 Euro wurden diesem Wert gegenübergestellt und als vernachlässigbar gering eingestuft. Dabei beliefen sich die Kosten für das Rechenzentrum als Provider auf Personalkosten von 12.120 Euro für insgesamt 404 Arbeitsstunden im ersten Jahr, von welchen 136 Stunden Aufwand für einmalige Tätigkeiten wie administrative Aufgaben und den Aufbau der Infrastruktur Aufwendungen von 4.080 Euro verursachten. Personalkosten in Höhe von 8.040 Euro entstanden auch in den Folgejahren für die Wartung und Weiterentwicklung der Gegenmaßnahmen sowie Support, welche mit 268 Stunden pro Jahr veranschlagt wurden. Die Kosten für Hard- und Software beschränkten sich auf jene für die Anschaffung eines neuen Servers für 3.000 Euro, die *„Open Source Software“ SpamAssassin* hingegen verursachte keine Kosten. Auch gaben von den Teilnehmern der Studie lediglich elf Befragte eine Summe von 536 Euro für Software zur Spam-Filterung aus, die große Mehrheit griff auf kostenlose Lösungen zurück.

Neben Fragen nach Arbeitszeitverlusten wurden in der Studie viele Angaben mit Hilfe einer 5-Punkte-Likert-Skala erfragt, um weitere Kostentreiber identifizieren zu können. So wurde von ungefähr der Hälfte der Befragten die Veröffentlichung der E-Mail-Adresse auf Webseiten vermieden, der Wert stieg dabei signifikant von 2,87 auf 3,28. Dagegen verzichtete mit 1,21 bzw. 1,31 in beiden Wellen eine überwältigende Mehrheit auf die Verwendung

ungewöhnlicher E-Mail-Adressen. Die Überprüfung potentieller Spam-Mails erfolgte bei den Probanden relativ einheitlich, so erreichten die Begutachtung des Absenders einerseits sowie der Betreff-Zeile andererseits Werte von 4,70 bzw. 4,71, das Öffnen der E-Mails hingegen nur 1,65. Eine Veränderung im Verhalten der E-Mail-Nutzung wurde ebenfalls untersucht, hier ergab sich für die reduzierte E-Mail-Nutzung wegen Spam ein Wert von 1,25, so dass sich nur ein geringer Anteil der Befragten von diesem Kommunikationsmittel zurückgezogen hat. Auch geben Clement et al. an, dass das Vertrauen in das Medium E-Mail durch Spam mit 2,24 bei der Minderheit gesunken ist und dass sich diese Vertrauensbasis in der zweiten Welle sogar minimal verbessert hat.

Der Wissensstand in Bezug auf Spam war ebenfalls Gegenstand der Untersuchung und ergab, dass die Mehrheit der Befragten ihre E-Mail-Adresse an Bekannte weitergaben, bei der Verbreitung an Unbekannte war das Verhalten sehr unterschiedlich. Etwa drei Viertel gaben an, ihre Adresse auf Webseiten oder in Online-Verzeichnissen hinterlegt zu haben, dagegen gab nur jeder Zehnte sie in Internet-Foren an. Nutzten in der ersten Welle noch 51,6 % einen (oder mehrere) Spam-Filter, so waren es ein Jahr später schon 67,7 %, insgesamt hatten 42,3 % ihre Schutzmaßnahmen ausgeweitet.

Die Verbreitung der eigenen Mail-Adresse an Unbekannte identifizierten Clement et al. (2008) neben der Anzahl empfangener Werbe-Mails als einen zentralen Kostentreiber. Bei der Untersuchung wurde eine Unterteilung der Befragten in zwei Segmente vorgenommen, von welchen das größere Segment S_1 66,6 % der Teilnehmer umfasste, das kleinere Segment S_2 dementsprechend 33,4 %. Im größeren Segment hielten sich die Arbeitszeitverluste mit mittleren 475 Minuten im Rahmen, während sich diese im zweiten Segment auf durchschnittlich 3.302 Minuten beliefen. Die mittlere Anzahl der Spam-Mails entwickelte sich in den beiden Befragungswellen in den beiden Segmenten gegenläufig, so stieg im ersten Segment diese Zahl von 9,92 auf 10,86 Spams pro Tag an, im kleineren Segment sank der Wert deutlich von ursprünglich 40,21 auf 31,85 Spam-Mails täglich. Clement et al. fassen zusammen, dass die Belastung durch Spam bei den Nutzern, welche mit einem besonders hohen Spam-Aufkommen konfrontiert gewesen waren, erheblich abgenommen hat, während die Spam-Menge für die restlichen Befragten gestiegen ist.

Vorbeugende Maßnahmen reduzierten nach Aussage der Autoren die Arbeitszeitverluste nur teilweise, eine Steigerung der Kosten wird indes durch die umfangreiche Überprüfung der E-Mails verursacht. Außerdem merkten Clement et al. an, dass die wahrgenommene Reaktanz auf die Belästigung durch Spam zu einem Vertrauensverlust in das Medium führe, welcher wiederum Kosten verursache. Kein signifikanter Einfluss wurde hingegen bei der Spam-Empfindlichkeit entdeckt, also den subjektiven Kriterien bei der Klassifikation beispielsweise von Witz-Mails als Spam. Daraus wurde in dem Artikel geschlussfolgert, dass Spam also nicht ein Problem der Wahrnehmung eines Mail-Nutzers sei, sondern unabhängig von der individuellen Definition gleichermaßen alle Mitarbeiter betroffen habe. Des Weiteren stellten die Autoren fest, dass ein Spam-Filter erst ab einem gewissen Volumen eine Kostenreduktion nach sich ziehe und somit individuell für besonders belastete Mitarbeiter einzusetzen sei.

Auch auf die Unterschiede zwischen den Nutzern, welche vor der ersten Befragungswelle schon einen Spam-Filter installiert hatten, und jenen ohne Schutzmaßnahmen wurde in dem Aufsatz eingegangen. Dabei ergaben sich für die Befragten mit Spam-Schutz zeitliche Kosten von 1665 Minuten gegenüber 734 Minuten investierter Zeit von Nutzern ohne Filter. Als Grund vermuteten die Autoren, dass sich diese Teilnehmer durch die hohen Kosten, welche durch ihre hohe Spam-Belastung verursacht wurden, dazu gezwungen sahen, einen eigenen Spam-Filter einzurichten. Diese Annahme konnte zwar durch die vorliegenden Daten nicht gestützt werden, der umgekehrte Schluss, ein Spam-Filter lasse die Kosten steigen, ergäbe jedoch auf der anderen Seite keinen Sinn. Auch habe der Vergleich der Daten beider Wellen gezeigt, dass die Befragten, welche bereits zum Zeitpunkt der ersten Welle einen Filter installiert gehabt hatten, in der zweiten Befragung mit erheblich niedrigeren Kosten konfrontiert gewesen waren.

Zusammenfassend empfahlen Clement et al. (2008) die Einrichtung eines zentralen Systems zur Filterung der E-Mails, sei es durch das Abblocken über eine *Blacklist* oder die Vorstufe der Filterung durch Kennzeichnung verdächtiger E-Mails ohne tatsächliches Aussieben von Spam-Mails. So seien die geringen Kosten im Rechenzentrum ein Indiz dafür, dass die Umsetzung einer solchen Lösung in einer zentralen Instanz am Effizientesten ist.

2.3 Theoretische Überlegungen

Wie bereits von Clement et al. (2008) geschildert wurde, gibt es im Bereich der Schätzung der durch Spam verursachten Kosten noch einen Mangel an verlässlichen Studien, eine solche Forschungslücke liegt auch für die Untersuchung der durch Schadprogramme entstandenen Kosten vor. Nun stellt sich natürlich die Frage, warum es in diesem Bereich bislang so wenig seriöse Untersuchungen gegeben hat, immerhin liegt die erste Virenpandemie inzwischen zehn Jahre zurück. So gab es zwar seit *Melissa* zahlreiche Publikationen, in denen der Versuch unternommen wurde, Zahlenwerte für die Schäden durch Viren, Würmer und Trojaner *anzugeben,* der Weg zu diesen Schätzungen bleibt dem Leser jedoch zumeist vorenthalten oder er entbehrt jeglicher wissenschaftlicher Grundlage. Viele von Unternehmensberatungen als Studien bezeichnete Veröffentlichungen sind jedoch für Kunden bestimmt, denen ein bestimmtes Produkt – und sei es nur die Studie selbst – verkauft werden soll und nicht für Wissenschaftler, deren kritischen Augen sie meistens nicht standhalten würden. Hier dürfte auch der Grund zu finden sein, warum diese Ergebnisse teilweise erheblich divergieren, in einigen Fällen kann sogar nicht einmal anhand des Textes nachvollzogen werden, welche Kosten berücksichtigt wurden und auf welche Region sich die Zahlen beziehen.

Die Schätzung der Kosten, die einerseits durch Schadprogramme und andererseits durch unerwünschte E-Mails verursacht werden, erweist sich zugegebenermaßen als ein sehr komplexes Problem. Sollen die volkswirtschaftlichen Kosten dieser beiden Facetten der Kriminalität im Internet geschätzt werden, so gilt es, eine Vielzahl von Faktoren zu berücksichtigen, viele dieser Faktoren besitzen die Eigenschaften von Opportunitätskosten. Neben den Ausgaben, welche für die Anschaffung von Software auf Unternehmen, öffentliche Einrichtungen und Privatpersonen zukommen können, fallen teilweise auch Kosten für Hardware an, beispielsweise für die Sicherheits-Infrastruktur von IT-Dienstleistern. Des Weiteren ergeben sich aus den Personalkosten für Administratoren, deren Arbeitskraft ohne die Existenz von Malware und Spam anderweitig eingesetzt werden könnte, weitere Kosten für Arbeitgeber. Die Produktivität dieser Fachleute könnte sinnvoller genutzt werden und geht gewissermaßen verloren.

Auch die Entwickler von Anti-Viren-Programmen könnten ihre Arbeitszeit in andere Projekte investieren und somit der Gesellschaft mehr Nutzen bringen, als sie es unter den gegebenen Umständen mit ihrer Arbeit tun. Doch wie ist die Zeit der Malware-Programmierer zu bewerten, die teilweise ebenfalls hochqualifizierte IT-Experten sind. Und sind den Kosten, die durch unerwünschte kommerzielle E-Mails verursacht werden, die Erlöse gegenüberzustellen, welche durch diese Werbemaßnahmen erst ermöglicht werden? Auch bliebe zu diskutieren, wie die Zeit zu bewerten wäre, die von Privatpersonen in ihrer Freizeit in den Kampf gegen Malware und Spam eingesetzt wird.

Auf den ersten Blick erscheint es einfacher, die Aufwendungen zu erheben, die ein Unternehmen im Kampf gegen Schadprogramme sowie unerwünschte E-Mail-Werbung aufzubringen hat. So lassen sich die Kosten quantifizieren, welche durch die Beschaffung von Hard- und Software verursacht werden, ebenso wie die Personalausgaben für Mitarbeiter, deren Aufgabe der Schutz vor diesen Bedrohungen aus dem Internet ist. Während Anti-Viren-Programme üblicherweise nicht frei verfügbar sind und somit zumindest im kommerziellen Umfeld bezahlt werden müssen, kann Software zur Spam-Filterung häufig kostenlos beschafft werden. Im Gegenzug entstehen jedoch bei Spam Kosten durch neue Hardware, wenn zur Filterung leistungsstärkere Server oder zur Speicherung größere Festplatten gekauft werden müssen. Des Weiteren wird auch mehr Bandbreite zur Bewältigung des wachsenden Mail-Volumens von Telekommunikationsdienstleistern nicht unentgeltlich zur Verfügung gestellt.

Kosten entstehen aber nicht nur durch die Beschaffung technischer Ausstattung, sondern auch durch deren Verwendung, da Hardware für ihren Einsatz konfiguriert werden muss und Software installiert sowie durch Updates auf dem neuesten Stand gehalten werden muss. Auch Betriebssysteme müssen in unregelmäßigen Abstanden durch Patches aktualisiert werden, woraus Kosten für Arbeitszeit resultieren, wenn statt dem vollautomatischen ein selektives Installieren der Patches gewünscht ist.

Doch nicht nur die Arbeitszeit von Administratoren verursacht Kosten, sondern auch der Zeitverlust aller Mitarbeiter, welcher beim Löschen oder gar Lesen von Spam-Mails und nicht zuletzt durch die Suche nach False Positives entsteht. Darüber hinaus werden bei Hoaxes nicht nur die betroffenen

Anwender, sondern auch Administratoren von produktiver Arbeit abgehalten, wenn verunsicherte Mitarbeiter aus Angst vor Malware-Befall einen (Fehl-) Alarm auslösen. Gerade in Bezug auf die Filterung von unerwünschten E-Mails hat die Studie von Clement et al. (2008) gezeigt, wie wichtig eine zentrale Einrichtung und Betreuung der Filtermaßnahmen ist und dass die dezentrale Spam-Filterung aus Kostengründen wenig Sinn ergibt. So sollten die Filterregeln an einer zentralen Stelle gepflegt und an aktuelle Veränderungen der Eigenschaften von Spam-Mails angepasst werden, um den Verlust an Arbeitszeit zu minimieren.

Schwieriger gestaltet sich hingegen die Schätzung der Kosten, welche durch Malware-Vorfälle verursacht werden, da hier Kosten für (unzureichende) Schutzmaßnahmen mit solchen für die Behebung der entstandenen Schäden zusammentreffen können. So müssen sich Administratoren umgehend um die Säuberung der befallenen Systeme kümmern und ihre anderen Aufgaben hinten anstellen, bei größeren Infektionen geht dies nicht selten mit Überstunden einher, welche dann zu zusätzlichen Kosten führen können. Ein nicht zu unterschätzender Faktor sind Produktivitätsverluste durch Ausfallzeiten, wenn infizierte Rechner nicht verfügbar sind und somit von den Anwendern nicht genutzt werden können. Diese Einbußen an Produktivität dürften den größten und am schwierigsten zu bestimmenden Anteil am Kostenpotential ausmachen, da hier durch den vorübergehenden Ausfall der IT-Infrastruktur der Produktionsablauf stillstehen und die Arbeit ganzer Abteilungen zum Erliegen kommen kann. Zuletzt sollte dann nach einem Malware-Vorfall eine Schwachstellenanalyse durchgeführt werden, um die Ursache für die Störung identifizieren zu können und durch Präventionsmaßnahmen weitere gleichartige Zwischenfälle zu vermeiden. Für diese Analyse könnte es dann sinnvoll sein, sich zur Beratung Hilfe von externer Seite zu suchen, wodurch erneut Ausgaben verursacht werden.

Weitere Aufwendungen könnten überdies vermieden werden, wenn Administratoren keine Fortbildungsveranstaltungen über Schutzmaßnahmen gegen Malware oder Spam besuchen müssten. Auch könnten Unternehmen Geld einsparen, wenn die Schulung von Anwendern im Umgang mit den Gefahren aus dem Internet oder zumindest ihre Aufklärung über diese Bedrohungen nicht nötig wären.

Die vorliegende Arbeit baut auf einer Studie auf, aus welcher die betriebswirtschaftlichen Kosten hervorgehen sollen, die deutschen Unternehmen jährlich durch Malware und Spam-Mails entstehen. Die methodischen Grundlagen für die zugrunde gelegte Umfrage werden in Kapitel 3 erörtert, die Vorgehensweise bei der Entwicklung des Fragebogens zur Erhebung der Daten folgt in Kapitel 4.

Bei der in dieser Untersuchung verwendeten *Contingent Valuation* Methode, welche in Abschnitt 3.2 detailliert vorgestellt wird, steht jedoch nicht die konventionelle Erhebung entstandener Kosten, deren Quantifizierung mit den geschilderten Problemen einhergeht, im Mittelpunkt. Vielmehr geht es um die Feststellung der Zahlungsbereitschaft für eine Dienstleistung zur Vermeidung dieser Kosten. Es bedarf keiner ausführlichen Erklärung, dass diese Zahlungsbereitschaften bei großen Unternehmen höher ausfallen dürften als bei kleinen und mittleren Betrieben. Offen bleibt jedoch zunächst, welcher Indikator der Unternehmensgröße diese Zahlenwerte maßgeblich beeinflusst, so könnten umsatzstarke Unternehmen zu höheren Zahlungen bereit sein als Firmen mit geringem Jahresumsatz. Andererseits könnte auch ein kleiner Personalbestand hohe Umsätze erzielen, so dass die Zahl der Mitarbeiter oder vielmehr die Zahl der zu schützenden Computer ausschlaggebend sein könnte. In diesem Fall wäre noch zu überprüfen, ob bei Unternehmen mit großer Mitarbeiterzahl Skaleneffekte zu erkennen sind.

Gerade im Zusammenhang mit Zahlungsbereitschaften stellt sich jedoch die Frage, ob diese wirklich bei den Opfern von Malware und Spam höher ausfallen, oder ob nicht eher das Investitionsverhalten in IT-Sicherheit in den geäußerten Werten abgebildet wird. Sind also Unternehmen bereit, mehr zu bezahlen, wenn sie (wiederholt) Vorfälle durch Malware hatten oder unter einer besonders hohen Spam-Quote leiden? Oder spiegeln sich die gehäuft auftretenden Malware-Probleme in unzureichenden Geldmitteln für Schutzmaßnahmen wieder, so dass aus mangelnder Investitionsbereitschaft geringere Zahlungsbereitschaften in der Umfrage resultieren. Unzweifelhaft dürften hingegen die befragten Unternehmen beim Kampf gegen Schadprogramme zu höheren Zahlungen bereit sein als bei der Reduzierung des Spam-Aufkommens, da unerwünschte E-Mails zwar Arbeitszeitverluste bedeuten, im Gegensatz zu Malware jedoch keine Ausfallzeiten verursachen. Auch ist

davon auszugehen, dass die Kosten von Spam in der Umfrage niedriger ausfallen sollten als bei Clement et al. (2008), da dezentrale Maßnahmen gegen Spam ineffizient und damit zu zeitaufwändig und kostenintensiv sind.

Im Rahmen der Erhebung des Datensatzes, welcher der Studie zugrunde liegen wird, soll auch gefragt werden, ob und in welchen Jahren die Probanden konkrete Vorfälle durch Viren, Würmer und Trojaner gehabt haben. Sofern die Frage zu diesem heiklen Thema in einer ausreichend großen Anzahl beantwortet wird, lässt sich möglicherweise zeigen, ob die teilnehmenden Unternehmen, bei denen bisher solche Zwischenfälle aufgetreten sind, im Antwortverhalten von den Zahlungsbereitschaften jener Unternehmen abweichen, die bislang virenfrei geblieben sind. Dann wäre es auch möglich, potentielle Ursachen oder Auswirkungen von Virenbefall zu entdecken und zu untersuchen, wie sich Opfer von Schadprogrammen von Betrieben unterscheiden, deren Schutz vor Malware ausreichend zu sein scheint. Es ließe sich untersuchen, ob es für Vorfälle und ihre Häufigkeit signifikant einflussnehmende Variablen gibt, oder ob Vorfälle durch Malware – abgesehen vom Einfluss der Schutzvorkehrungen – ein Produkt des Zufalls sind. Letzten Endes könnte auch festgestellt werden, ob es immer wieder die gleichen Unternehmen trifft, welchen Einfluss die Investitionsbereitschaft in IT-Sicherheit hat und ob Firmen, die E-Commerce nutzen oder gar selbst anbieten, besser geschützt und damit weniger betroffen sind.

Bei den Unternehmen, die sich von externer Seite im Bereich IT-Sicherheit beraten lassen oder ihre IT-Aufgaben teilweise oder vollständig ausgelagert haben, sind dabei mehrere, unterschiedlich zu interpretierende Ergebnisse denkbar. So könnten auf der einen Seite Unternehmen, die sich beraten lassen, als Ergebnis einer guten Beratung weniger Vorfälle durch Schadprogramme haben, auf der anderen Seite könnten sie aber auch häufiger Malware-Befall gehabt haben und sich in der Zwischenzeit als Reaktion darauf Hilfe von außen gesucht haben. Allerdings konnte im Vorfeld der Studie nicht eingeschätzt werden, wie bereitwillig die Teilnehmer über ihre spezifische Malware-Situation Auskunft geben werden, da das Bekanntwerden von Schwachstellen im Bereich IT-Sicherheit einen Vertrauensverlust von Investoren und Kunden zur Folge haben könnte. Schließlich stellt sich bei Sicherheitslücken die Frage, ob die Daten eines Unternehmens mit Malware-Problemen noch vor dem

unbefugten Zugriff Dritter sicher sind. Insofern blieb abzuwarten, inwieweit die Unternehmen auf die Seriosität der Umfrage und die damit verbundene zugesicherte Anonymität ihrer Angaben vertrauten und sich dazu durchringen konnten, die Karten auf den Tisch zu legen.

Die Frage nach dem Spam-Anteil am täglichen E-Mail-Aufkommen hingegen dürfte sich weniger problematisch gestalten, hierüber geben Unternehmen vermutlich offener Auskunft als über Schäden durch Schadprogramme. Während das Eingestehen von Vorfällen durch Malware, wenn hierfür mangelhafte Vorkehrungen für IT-Sicherheit als Grund angenommen werden, eher dem Ruf schaden könnte, scheint Spam in der öffentlichen Wahrnehmung ein allgemein akzeptiertes Problem zu sein. Somit dürfte sich diese Frage in puncto Antwortverhalten als unkritisch erweisen und eine ausreichend große Anzahl an Beobachtungen für Schätzungen im Zusammenhang mit dieser Variable möglich sein. Sollte zusätzlich der Fragenblock zu Vorfällen durch Viren, Würmer und Trojaner gut beantwortet worden sein, so ließe sich auch untersuchen, ob es eine Verbindung zwischen Malware-Befall und dem Anteil der Spam-Mails am Mail-Verkehr eines Unternehmens gibt.

Als letzte Fragestellung sollten noch die wichtigsten Indikatoren identifiziert werden, für die ein signifikanter Zusammenhang mit der Entscheidung für oder gegen IT-Beratung sowie den Grad des Outsourcings von IT-Verantwortlichkeit festgestellt werden kann. In diesem Fragenbereich ist eine starke Verknüpfung zwischen IT-Beratung und der Fremdvergabe von IT und IT-Sicherheit zu erwarten, da die beiden Konzepte über eine große inhaltliche Schnittmenge verfügen. Daher soll überprüft werden, ob es diesen vermuteten Zusammenhang gibt und welche weiteren Variablen als Auslöser oder Folge der jeweiligen Entscheidung in Frage kommen, so ist hier ein Bezug zur Personalzusammensetzung ebenso denkbar wie zu der Bereitschaft, Mitarbeiter weiterzubilden.

Nachdem in den hier entwickelten Hypothesen vermehrt von *Zahlungsbereitschaften* gesprochen wurde und der Begriff der *Kosten* bei der Wortwahl immer mehr in den Hintergrund gerückt ist, wird im folgenden Kapitel ausführlich auf die *Contingent Valuation* Methode eingegangen. Im Rahmen der Vorstellung der eingesetzten Methoden werden Kritikpunkte und Schwächen sowie Vorteile und Stärken dieses Ansatzes aufgeschlüsselt.

Kapitel 3

Methodik

Um die Kosten von bestimmten Teilaspekten der IT-Sicherheit zu schätzen, werden viele Informationen benötigt, welche teilweise nicht *a priori* zur Verfügung stehen. Doch um beispielsweise Investitionen in Schutzmaßnahmen gegen Schadprogramme rechtfertigen zu können, muss bei der Entscheidung der Finanzierung die Rentabilität der Maßnahme(n) gegeben sein. In diesem Kapitel werden zunächst Modelle zur Schätzung der Kosten von IT-Sicherheit betrachtet, welche teilweise in der Praxis umgesetzt werden, im Rahmen dieser Arbeit jedoch aus den im Folgenden geschilderten Gründen nicht zum Einsatz kamen.

Auf die kennzahlenbasierten Ansätze folgt dann in Abschnitt 3.2 mit der *Contingent Valuation* Methode die Diskussion eines präferenzbasierten Bewertungsansatzes. Diese Methode wurde zwar bereits wiederholt in der Kriminometrie eingesetzt, findet aber im Rahmen dieser Arbeit erstmalig Anwendung in der Schätzung von Kosten für IT-Sicherheit. Mit Hilfe der *Contingent Valuation* Methode sollen dann in den folgenden Kapiteln die Kosten von unerwünschten E-Mails sowie von Schadprogrammen geschätzt werden.

Zum Ende des Kapitels werden mit der Faktoren- und einer speziellen Form der Regressionsanalyse sowie einem Variablenauswahlverfahren die für die Analysen der erhobenen Daten verwendeten multivariaten Verfahren vorgestellt.

3.1 Kennzahlenbasierte Schätzansätze

Bei der Identifizierung der „Kosten und Kostentreiber“ von Spam-Mails berechneten M. Clement et al. (2008) die durch unerwünschte E-Mails verursachten Kosten anhand der (Arbeits-)Zeit, welche von Mitarbeitern der Universität Kiel in die Bekämpfung der elektronischen Belästigung investiert wurde. Bei der Schätzung der Kosten von Malware und Spam über Arbeitszeitverluste tritt das Problem auf, dass Produktivitätseinbußen nur ein Teilaspekt der komplexen Kostenstruktur sind, welche durch die unerwünschten Effekte der Internet-Anbindung verursacht werden. Doch viele Kosten können auf diese Weise gar nicht genau erfasst werden, so dass es sich als sehr schwierig erweist, die gesamten Kosten zu berechnen.

Die Kosten für die Anschaffung und Betreuung eines Servers zur vorgeschalteten Filterung von Spam-Mails mögen zudem für große Betriebe nur geringe Kosten pro Mitarbeiter verursachen, gerade für kleinere Unternehmen liegen diese Kosten in Relation zur Mitarbeiterzahl aber erheblich höher. Insofern bietet sich für kleinere Betriebe das Auslagern solcher Schutzmaßnahmen an externe Dienstleister eher an, um die relativen Kosten gering zu halten.

Gerade bei den durch Schadprogramme verursachten Kosten ist allerdings zu beachten, dass der Umfang der Ausfallzeiten zum einen nicht vorhersehbar ist, und zum anderen auch nur einen Teil der Kosten abbildet, die durch einen Vorfall entstehen können. In der Praxis wurde daher beispielsweise mit dem *Return on Security Investment* eine Methode eingeführt, um sich eine Möglichkeit zu schaffen, auf Basis einer Kennzahl die Kosten eines Malware-Vorfalls zu schätzen.

Die Stärken und Schwächen dreier solcher kennzahlenbasierter Schätzansätze, die sich prinzipiell für die Berechnung der Kosten von Spam und Malware eignen könnten, werden in diesem Abschnitt beleuchtet und kurz diskutiert. Diese Ansätze entstammen durchweg der unternehmerischen Praxis und wurden bereits zur Schätzung der Rentabilität von Kapitaleinsatz oder der Einschätzung risikobehafteter Investitionen angewendet.

3.1.1 Return on Investment (ROI)

Der *Return on Investment (ROI)* oder *Rate of Return (ROR)*[1] ist der Quotient aus Gewinn bzw. Verlust einer Investition und eingesetztem Kapital und wird im Deutschen auch als Gesamtkapitalrentabilität oder Kapitalrendite bezeichnet. Der 1919 von Donaldson Brown eingeführte ROI ist im vom Chemiekonzern DuPont de Nemours entwickelten Kennzahlensystem als das Produkt aus Umsatzrendite und Kapitalumschlag definiert[2] und dient zur Messung der Rendite des Gesamtkapitals. Die Kennzahl aus der Rentabilitätsrechnung ist ein Anteilswert ohne Einheit und wird meistens in Prozent angegeben.

Der Definition nach impliziert der ROI keine Laufzeit der Investition, er wird jedoch häufig auf ein (Kalender- bzw. Geschäfts-)Jahr heruntergebrochen. Ebenso betrachtet der *Return on Investment* nach Browns ursprünglicher Definition im Du-Pont-Kennzahlensystem *(„DuPont System of Financial Control“)* die Rentabilität des gesamten in einem Unternehmen gebundenen Kapitals, eine erweiterte Auslegung erlaubt jedoch auch die Bewertung einzelner Investitionen. Die Kapitalrendite kann daher herangezogen werden, um Investitionen gesondert zu bewerten und vergleichbar zu machen, da mit ihr nicht absolute Ergebnisse, sondern relative Gewinne ausgewiesen werden.

Da der *Return on Investment* auf der Gewinn- und Verlustrechnung und der Bilanz basiert, ist er eine *ex post* Betrachtung der Kapitalrentabilität, diese Orientierung an der Vergangenheit steht ebenso in der Kritik wie die fehlende Einbeziehung zukünftig zu erwartender Entwicklungen. Auch ist eine *ex ante* Einbeziehung der Risikowahrscheinlichkeit für Investitionen im ursprünglichen Konzept des *Return on Investment* nicht vorgesehen, die für eine Berechnung zukünftiger Kosten und Erlöse notwendig wäre.

[1] Weitere Bezeichnungen in der Literatur sind unter Anderem *Rate of Profit* oder nur *Return.*

[2] Da Umsatzrendite $= \frac{\text{Gewinn}}{\text{Umsatz}} \times 100$ und Kapitalumschlag $= \frac{\text{Umsatz}}{\text{Kapitaleinsatz}}$ ist, entspricht die Definition dem erweiterten Quotienten aus Gewinn und Gesamtkapital in Prozent.

3.1.2 Return on Security Investment (ROSI)

Der *Return on Security Investment (ROSI)* wurde entwickelt, um Ausgaben für IT-Sicherheit in Budgetgesprächen durch Angabe einer Kennzahl rechtfertigen zu können. Dabei lassen sich theoretisch für einzelne Projekte Kosten und Nutzen analysieren und anhand des eingesetzten Kapitals bewerten. Ein großes Problem der IT-Sicherheit im Allgemeinen ist aber, dass die durch ihren Einsatz vermiedenen Folgen üblicherweise den Charakter von Opportunitätserlösen besitzen. In diesem Fall wird die Entstehung realer Kosten beispielsweise durch das Verhindern von Virenbefall unterbunden, folglich ist es schwer, die hypothetischen Kosten eines Malware-Vorfalls zu quantifizieren.

Abweichend vom namensverwandten *Return on Investment* wird jedoch der *Return on Security Investment* nicht als Quotient von Gewinn bzw. Verlust und Kapital, sondern als Differenz von Schadenssenkungspotential und Kosten der Schutzmaßnahme berechnet. Der ROSI ergibt somit einen absoluten Geldbetrag, der bei positivem Vorzeichen eine rentable Investition implizieren soll.

Im Allgemeinen gestaltet sich die Berechnung des *Return on Security Investment* aufgrund der (Nicht-)Messbarkeit des Schadenssenkungspotentials schwierig, weil die Investitionen unter Unsicherheit getätigt werden. Deswegen wies J. Schoolmann (2005) darauf hin, dass der ROSI nicht wirklich der Stärkung der Budget-Argumentation diene, da die Kostenersparnis weiterhin geschätzt werden müsse. So entzögen sich Sicherheitsbetrachtungen auch faktisch einer ROI-Berechnung und machten damit auch den *Return on Security Investment* als (alleinige) Entscheidungsgrundlage ungeeignet. Anhand von zwei kurzen Beispielen aus der Praxis zeigten K. Schmeh und H. Uebelacker (2004) aber, dass es im Einzelfall doch möglich ist, die IT-bezogene Kennzahl einer Investition zu berechnen, wenn auch nur *ex post* und ohne Unsicherheit.

Bei einem der Beispiele handelte es sich um den Einsatz von *„Single Sign-On“*-Systemen *(SSO)* [sic!], bei denen sich ein Benutzer nur einmal authentisieren muss, sei es durch Eingabe eines Passworts oder unter Verwendung einer sogenannten Smartcard. Im konkreten Fallbeispiel hatte eine Bank mit

30.000 Anwendern vor der Umstellung auf SSO monatlich ca. 30.000 passwortbezogene Anrufe beim Helpdesk zu beklagen, schon in kurzer Zeit konnte die Zahl dieser Anrufe um mehr als ein Drittel reduziert werden, mit weiterhin fallender Tendenz. Über den Produktivitätsausfall von durchschnittlich 20 Minuten je Anruf und einen Stundensatz von 60 Euro wurde auch ohne die Berücksichtigung der Entlastung des Helpdesk ein Einsparungspotential von 2,4 Mio. Euro errechnet. Während eine tatsächliche Produktivitätssteigerung durch die Zeitersparnis nicht nachgewiesen wurde, konnte ein Erfolg jedoch eindeutig belegt werden, und zwar die gestiegene Zufriedenheit der Anwender mit der IT.

Die Berechnung einer Rendite für die Investition in Schutzmaßnahmen gegen Malware scheitere laut Mummert Consulting (2003) häufig am Fehlen zuverlässiger Daten über Schadenshäufigkeiten und Schadenshöhen, dazu komme, dass sich die Kalkulation von Ausfallzeiten und den daraus resultierenden Kosten allgemein sehr aufwändig gestalte. Daher sei die Ermittlung der notwendigen Daten für kleinere Betriebe oftmals schwer und wegen des Aufwands unrentabel, große Unternehmen hingegen können die benötigten Statistiken für die Modellrechnung meistens zur Verfügung stellen. Zudem wurde angemerkt, dass für viele IT-Sicherheit nur Kosten aufweise, da ein *Return on Security Investment* kaum berechnet würde, so sähen nach der (weltweit durchgeführten) Studie „IT-Security 2003“ nur 15 % der 2.461 teilnehmenden Unternehmen einen Zusammenhang zwischen Gewinn und IT-Sicherheit.

Durch die täglich steigende Anzahl im Internet kursierender Schadprogramme und die Jahr für Jahr verbesserten Verbreitungsmethoden lassen sich nur schwer Szenarien schaffen, in denen die Wahrscheinlichkeit eines Malware-Vorfalls mit all seinen (technischen und finanziellen) Folgen realistisch abgebildet werden kann. Die Simulation eines solchen Szenarios wird erschwert durch die Tatsache, dass nach einer Initialinfektion durch das heutzugetage übliche Ausschalten der Sicherheitsvorkehrungen auf dem befallenen Rechner weiteren Schadprogrammen Tür und Tor geöffnet wird.

In einem Beispiel zeigten C. Abel und R. Thiele (2003) die Schwierigkeiten bei der Berechnung des *Return on Security Investment*, die Ermittlung erfolgte dabei in drei Schritten. Nach der Identifikation der zu schützenden

Informationsgüter und möglicher Präventionsmaßnahmen finde zunächst die Bewertung der Informationsgüter und des Risikos statt, bevor dann die Bewertung der Investition durch die Ermittlung des ROSI erfolge. Angenommen seien Kosten von 100.000 Euro für einen Virenbefall sowie eine Eintrittswahrscheinlichkeit von 30 % pro Jahr, der zu erwartende Verlust beliefe sich demnach auf 30.000 Euro. Senke nun ein Anti-Viren-Programm für 12.000 Euro die Schadenswahrscheinlichkeit um zwei Drittel, dann betrage das Schadenssenkungspotential 20.000 Euro, woraus ein neuer zu erwartender Verlust (im Schadensfall) von 10.000 Euro entstünde. Der (positive) *Return on Security Investment* beliefe sich im Beispiel auf 8.000 Euro und wäre somit eine lohnende Investition.

Bei der Präzisierung der einzelnen Schritte verdeutlichten Abel und Thiele aber, dass sich die Berechnung des ROSI nicht für jede Investitionsentscheidung eigne, und führten die wichtigsten Probleme bei der Ermittlung der Kennzahl an. So stoße man bei der Identifikation der Informationen, die für den Fortbestand des Unternehmens entscheidend oder weniger kritisch seien, bereits auf erste Probleme. Auch stütze sich die Ermittlung schwer messbarer Werte häufig auf Annahmen und Schätzungen, beispielsweise bei der Untersuchung von Schadenspotentialen oder Schadenssenkungspotentialen, ebenso müssten verschiedene Schadensszenarien abgebildet werden. Wichtig sei auch, nicht nur Einzelmaßnahmen zu betrachten, sondern auch die Interdependenzen zu evaluieren, da erst ein Gesamtkonzept die volle Ausschöpfung des Potentials der einzelnen Maßnahmen ermögliche. Schließlich sei besonders die Verwendung historischer Daten bei der Bewertung zukünftiger IT-Gefahren problematisch, darüber hinaus gebe es auch nicht messbare positive Effekte, die nicht in den ROSI einfließen können.

Alles in allem erweist sich die Verwendung des *Return on Security Investment* als schwierig, da er nur für ausgewählte Szenarien sinnvoll als Entscheidungshilfe herangezogen werden kann. Gerade bei der Bewertung von Sicherheitsrisiken durch Schadprogramme müssen jedoch mit der Eintrittswahrscheinlichkeit und dem Schadenspotential des Malware-Vorfalls sowie dem Schadenssenkungspotential der Schutzsoftware aufgrund der ebenso unbekannten Schadensminderungswahrscheinlichkeit zu viele entscheidende Variablen geschätzt werden.

3.1.3 Value at Risk (VaR)

Der Begriff *„Value at Risk“ (VaR),* zu Deutsch Wert im Risiko, stammt aus dem Risikomanagement, also dem planvollen Umgang mit unternehmerischen Risiken im Allgemeinen, aber auch mit finanziellen Risiken. Die Risikokennzahl, deren Angabe in einer Währung erfolgt, gibt an, welcher maximale Verlust in einem gegebenen Zeitraum zu einem bestimmten Konfidenzniveau nicht überschritten wird. Beispielsweise bedeutet ein VaR von 1 Mio. Euro bei einem Zeithorizont von 10 Tagen und einem Konfidenzniveau von 99 %, dass ein Verlust von 1 Mio. Euro innerhalb der nächsten 10 Tage mit einer Wahrscheinlichkeit von 99 % nicht überschritten wird. Implizit liegt also die Wahrscheinlichkeit, mehr als 1 Mio. Euro innerhalb dieser Zeit zu verlieren, unter einem Prozent.

Der von JPMorgan Chase & Co. entwickelte *Value at Risk* ist heute ein Standardrisikomaß im Finanzsektor und wird in Unternehmen zur Bewertung zumeist finanzwirtschaftlicher Risiken verwendet. Während das Konzept bereits Ende der 80er Jahre entstanden war, wurde der Begriff *„Value at Risk“* erst im Jahr 1993 geprägt. Das Risikomaß wird bevorzugt zur Quantifizierung und Steuerung von Marktpreisrisiken im Rahmen von Basel II[3] eingesetzt.

Zur Schätzung des *Value at Risk* können verschiedene Modelle zugrunde gelegt werden, von denen jedes auf eigenen Annahmen basiert. Dabei ist eine häufige Annahme, dass historische (Markt-)Daten am besten für die Schätzung zukünftiger Veränderungen geeignet sind. Im Folgenden wird ein kurzer Überblick über die drei wichtigsten Ansätze gegeben.

Der „Varianz-Kovarianz-Ansatz“ entspricht dem ursprünglichen VaR-Ansatz und wurde im Jahr 1994 durch die Veröffentlichung des *„RiskMetrics Technical Document“* der JPMorgan-Bank bekannt. Der parametrisierte Ansatz, der korrekterweise als „Delta-Normal-Ansatz“ bezeichnet werden müsste, häufig aber synonym verwendet wird, basiert auf der Annahme, dass die Risikofaktoren einer gemeinsamen Normalverteilung unterliegen und Wertveränderungen linear abhängig von allen Risikofaktoren sind.

[3]Bei Basel II handelt es sich um Eigenkapitalvorschriften des Basler Ausschusses für Bankenaufsicht *(Basel Committee on Banking Supervision of the Bank for International Settlements),* die seit 2007 für alle Kredit- und Finanzdienstleistungsinstitute der EU-Mitgliedsstaaten anzuwenden sind.

Ein wichtiger Vorteil des Ansatzes ist, dass keine umfangreichen Datensätze für die Berechnung des *Value at Risk* benötigt werden, weiterhin erweist sich durch die Vorbedingung der Linearität die Berechnung als unkompliziert und sehr schnell, gerade die Annahme linearer Abhängigkeiten schränkt die Einsetzbarkeit des Delta-Normal-Ansatzes aber stark ein. Auf die Einschränkung auf lineare Modelle verzichtet beispielsweise der „Delta-Gamma-Ansatz“, die unterstellte Normalverteilung ist aber ein gemeinsamer Nachteil aller Varianz-Kovarianz-Modelle, da sie nicht der Verteilung realer Marktpreisänderungen entspricht.

Als konzeptuell sehr einfach erweist sich die „Monte-Carlo-Simulation“, welche jedoch unter den hier vorgestellten Ansätzen den meisten Rechenaufwand erfordert.[4] Hier wird nach der Festlegung einer Anzahl von Iterationen bei jedem Durchlauf ein zufälliges Marktszenario auf Basis eines gegebenen Marktmodells generiert, um durch die Neuberechnung des Portfolios unter den simulierten Umständen einen Gewinn oder Verlust zu berechnen. Dabei wird für die Simulation zumeist keine Verteilungsannahme getroffen, sondern eine kleine Stichprobe als Basis herangezogen. Nach der letzten Iteration werden die Ergebnisse sortiert, um die Verteilung der Simulation zu erhalten, anhand des Konfidenzniveaus n kann dann das $(100 - n)$-te Perzentil bestimmt werden. Die Monte-Carlo-Simulation eignet sich generell, um den VaR für Porfolios mit nicht-linearen Eigenschaften wie beispielsweise Optionen zu berechnen. Allerdings ist neben dem geringen Problem der Rechenintensivität als Nachteil anzumerken, dass im Falle einer nicht vorhandenen Stichprobe als Datengrundlage eine Verteilungsannahme getroffen werden muss.

Da die „Historische Simulation“ keine parametrisierten Modelle für die Risikofaktoren zugrunde legt, handelt es sich bei ihr um einen nicht-parametrisierten Ansatz. Dabei wird auf Basis historischer Marktdaten unterstellt, dass sich alle Risikofaktoren zukünftig wie in der Vergangenheit entwickeln. Eine gegebene Zahl von (vergangenen) Beobachtungen entspricht bei diesem Ansatz der entsprechenden Zahl zukünftiger Veränderungen, aus deren (empirischer) Verteilungsfunktion das entsprechende Perzentil und somit der *Value at Risk* abgeleitet werden kann. Der Vorteil dieser Vorgehensweise ist

[4] Bei der Rechenleistung aktueller Computer ist dieser Nachteil jedoch vernachlässigbar und wird lediglich der Vollständigkeit halber erwähnt.

neben der einfachen Implementation die Tatsache, dass den Entwicklungen am Markt keine Verteilung unterstellt werden muss. Auf der anderen Seite ist für diese Simulation eine umfangreiche Datenbank mit Marktdaten notwendig, um verlässliche Ergebnisse zu erhalten, des Weiteren sei erwähnt, dass sich auch diese Methode als sehr rechenintensiv erweist.

Ein häufiger Kritikpunkt des *Value at Risk* ist, dass zwar unter der Voraussetzung ausreichender Daten für das Modell der maximale Verlust zu einem gewählten Konfidenzintervall berechnet werden kann, ein maximal möglicher Verlust jedoch nicht bestimmt werden kann. Ein weiteres Problem des VaR ist, dass er nicht subadditiv[5] und damit kein kohärentes Risikomaß ist, auch wenn sich diese Eigenschaft nicht gravierend auf die Anwendbarkeit zur Bestimmung eines Marktpreisrisikos auswirkt.

Das Problem bei einem Einsatz des VaR-Ansatzes zur Berechung von möglichen Verlusten durch IT-Gefahren wie Malware ist, dass entweder eine Verteilungsannahme getroffen werden muss, oder umfangreiche Datensätze für die historische Simulation benötigt werden. Um beispielsweise eine Normalverteilung zu unterstellen, wird aber zumindest eine minimale Ausgangsstichprobe benötigt, um die Annahme ansatzweise unterlegen zu können. Insofern dürfte sich eine Verteilungsannahme sehr problematisch gestalten. Auch die historische Simulation dürfte sich gerade im Zusammenhang mit einem sich permanent weiterentwickelnden Phänomen wie den Schadprogrammen aufgrund ihrer Vergangenheitsorientierung wenig für die Vorhersage von zukünftigen Ereignissen eignen. Selbst wenn eine entsprechend umfangreiche Datenbasis zur Verfügung stünde, wäre aufgrund der Tatsache, dass es bei Schadprogrammen immer neue Entwicklungen gibt, eine zukunftsbezogene Aussage nur schwer zu treffen.

Zur separaten Abbildung der Malware-Situation unter Außerachtlassung weiterer Bedrohungen aus dem Internet kann ein einzelnes „Schadprogramm-Portfolio“, dessen Entwicklung mit dem *Value at Risk*-Ansatz prognostiziert werden soll, nicht ausreichen, denn Schadprogramme und ihr Zusammenspiel untereinander beim Befall eines Computers können nicht einmal ansatzweise als homogene Menge betrachtet werden. Viren, Würmer und Trojaner sind in

[5]Subadditivität liegt vor, wenn $V(a+b) \leq V(a) + V(b)$ gilt.

der Zwischenzeit so vielseitig, dass eine Unzahl von Szenarien durchexerziert werden müsste, um für das heterogene Portfolio eine annähernd realistische Risikoverteilung zu erhalten. Wird hingegen die Gesamtheit der Schadprogramme in verschiedene Portfolios aufgeteilt, in welchen Viren und Würmer anhand ihrer Eigenschaften in Gruppen zusammengefasst werden, tritt wieder das Problem der fehlenden Subadditivität des *Value at Risk* auf. Darüber hinaus stellt sich bei diesem Ansatz auch das Problem, die durch Schadprogramme verursachten Kosten zu quantifizieren.

Die realitätsnahe Abbildung eines so komplizierten Szenarios mit zukunftsorientierter Aussagekraft scheitert also letzten Endes nicht nur am Fehlen einer umfangreichen Datenbasis, sondern auch an der Komplexität des Phänomens „Malware“.

Wie gezeigt eignen sich die hier vorgestellten kennzahlenbasierten Schätzansätze nur bedingt zur Berechnung der Kosten, welche durch nicht vorhersehbare Ereignisse wie Vorfälle mit Malware oder das Spam-Aufkommen verursacht werden können. Aus diesem Grund wurde eine präferenzbasierte Bewertungsmethode in Betracht gezogen, welche in der Vergangenheit in den verschiedensten Bereichen der empirischen Forschung eingesetzt wurde und bereits wiederholt in der Schätzung der Kosten von Kriminalität zur Anwendung kam.

Der folgende Abschnitt diskutiert die *Contingent Valuation* Methode und analysiert die Probleme, die bei ihrer Verwendung auftreten können. Weiterhin gibt er einen Überblick über die Vorzüge, welche das Verfahren für eine Studie über die Kosten von IT-Sicherheit attraktiv erscheinen lassen, außerdem erfolgt eine genauere Betrachtung der kriminometrischen Untersuchungen. Die Überlegungen zum Design der Erhebung unter Beachtung der Schwächen der Methode folgen in Abschnitt 4.1.

3.2 Contingent Valuation Method (CVM)

Bei der *Contingent Valuation* Methode[6] *(CVM)* handelt es sich um ein umfragebasiertes Konzept zur ökonomischen Bewertung von Gütern, für die es keine Marktdaten gibt, oder die den Charakter eines öffentlichen Gutes besitzen. Paul R. Portney (1994, S. 3) leitete seinen Artikel zur Debatte über dieses Verfahren ein, indem er die grundlegenden Charakteristika der Methode umriss und im Folgenden erläuterte:

„The contingent valuation method involves the use of sample surveys (questionnaires) to elicit the willingness of respondents to pay for (generally) hypothetical projects or programs. The name of the method refers to the fact that the values revealed by respondents are contingent upon the constructed or simulated market presented in the survey.“

Demnach werden bei diesem Verfahren im Rahmen von Befragungen individuelle Zahlungsbereitschaften für üblicherweise hypothetische (aber auch tatsächlich erwogene) Projekte oder Programme erfragt. Ferner wies Portney darauf hin, dass die von den Probanden geäußerten Zahlungsbereitschaften von dem im Fragebogen dargestellten Marktszenario abhängig seien.

3.2.1 Der Ursprung der Contingent Valuation

Die theoretische Grundlage für die CVM schuf Siegfried von Ciriacy-Wantrup im Jahr 1947 mit seinem Aufsatz *„Capital Returns of Soil Conservation Practices“,* in welchem er als Erster die Methode zur Bestimmung der Nachfrage nicht handelbarer Güter vorschlug. In seiner Arbeit über den Nutzen der Verhinderung von Bodenerosion beobachtete er, dass einige positive Effekte, wie die reduzierte Verschlammung von Flüssen, teilweise den Charakter eines öffentlichen Gutes aufwiesen. In diesem Zusammenhang schlug Ciriacy-Wantrup die Befragung der Bevölkerung über ihre *„willingness to pay“ (WTP),* also ihre Zahlungsbereitschaft für die schrittweise Erhöhung der Verfügbarkeit eines solchen öffentlichen Gutes vor.

[6] Die *Contingent Valuation* Methode wird in der deutschen Literatur als „Kontingente Bewertungsmethode“ übersetzt.

Die praktische Umsetzung dieser Idee ließ jedoch noch 16 Jahre auf sich warten, bis R. Davis (1963) im Rahmen seiner Doktorarbeit versuchte, mittels einer Umfrage den Wert zu schätzen, den Jäger und Naturfreunde einem bestimmten Erholungsgebiet beimäßen. Die Resultate seiner CVM-basierten Umfrage verglich er mit einer Schätzung der auf der Reisekostenmethode[7] von H. Hotelling basierenden Zahlungsbereitschaft und stellte eine hohe Korrelation seiner Ergebnisse mit diesem etablierten Verfahren fest.

Der ökonomische Wert der Natur stand auch im Mittelpunkt des Aufsatzes *„Conservation Reconsidered“* von J. Krutilla (1967), in dem er aufschlüsselte, wie der hohe (ökonomische) Wert von Naturräumen durch infrastrukturelle Erschließung, beispielsweise zum Abbau von Bodenschätzen, verloren gehe. Dabei wies er sowohl auf den aktiven Nutzwert, wie beispielsweise als Erholungsgebiet, hin, als auch auf den „passiven“ Nutzen, den Menschen einem Gut beimäßen, obwohl sie dieses Gut nicht aktiv nutzten.[8]

Jener passive Nutzen, den Krutilla in diesem Zusammenhang etablierte,[9] wird aufgrund der Tatsache, dass die Existenz eines Gutes für den Einzelnen einen Wert haben kann, in der englischen Literatur als *„existence value“* oder *„non-use value“* bezeichnet. Des Weiteren erwähnte Krutilla bereits Ende der 60er Jahre, dass sich der aktive Nutzen eines Naturparks durch den technischen Fortschritt im Bereich der Outdoor-Aktivitäten durchaus dynamisch gestalten könne, wenn die Nachfrage nach Erholungsgebieten steige.[10] Im Gegensatz zu vom Menschen gefertigten Gütern könne nach Krutilla das Angebot an den Annehmlichkeiten der Natur sinken.

[7] Im Jahr 1947 wurde neben dem Kontingenten Bewertungsansatz von Ciriacy-Wantrup der Reisekostenansatz *(Travel cost analysis* oder *Travel cost method)* von Hotelling vorgestellt. Die beiden Methoden waren entwickelt worden, um latente Nachfragefunktionen für nicht marktfähige Güter bestimmen zu können. Bis dato war allgemein die Meinung vertreten worden, einem Gut, für das es keinen Marktpreis gäbe, könne kein ökonomischer Wert zugewiesen werden.

[8] So kann man beispielsweise dem Schutz des Regenwaldes im Amazonas (nicht nur im Rahmen des Erhalts unseres Ökosystems) einen gewissen Nutzen zusprechen und auch eine Zahlungsbereitschaft an den Tag legen, ohne tatsächlich zu planen, jemals nach Südamerika zu reisen.

[9] Krutilla selbst bezeichnete den Nutzen in seiner Arbeit als *„sentimental value“*.

[10] Das zwischenzeitlich entwickelte Mountainbike erhöhte die Nachfrage nach Gebieten, in denen man sie nutzen konnte, erheblich.

Dieser wegweisende Beitrag von Krutilla ebnete der *Contingent Valuation* Methode den Weg in der Nationalökonomie, insbesondere im Bereich der Ressourcen- und Umweltökonomik, in dem sie ihren Ursprung hat und seither auch schwerpunktmäßig eingesetzt wird. So führte eine Übersicht über die Verwendung der CVM von R. Carson et al. bereits im Jahr 1994(a) zu einer Auflistung von 1.674 Studien bzw. Veröffentlichungen.

Der erste Versuch, im Bereich der (Umwelt-)Politik Fuß zu fassen, misslang der *Contingent Valuation* Methode im Zusammenhang mit dem US-amerikanischen *„CERCLA act“*[11] Anfang der 80er Jahre. Zwar äußerte die US-Regierung Interesse an der Feststellung von *existence values* und somit am Einsatz der CVM, faktisch verhinderten jedoch die Ausführungsrichtlinien des zuständigen Innenministeriums deren Verwendung in den meisten Fällen. Ursprünglich wurde das als *„Superfund Law“* bekannte Gesetz geschaffen, um (aufgegebene) Sondermülldeponien aufzuspüren und zu beseitigen und es den Geschädigten zu ermöglichen, Schadensersatzansprüche gegen die Urheber geltend machen zu können. Durch die ministeriellen Bestimmungen wurde die CVM aber zumeist nur dann angewendet, wenn *„use values“* nicht messbar waren. Eine tatsächliche Bewertung der Schädigung der Natur fand daher sehr selten statt.

Erst im Jahr 1989 gelang der *Contingent Valuation* Methode der Durchbruch in der Wirtschaftspolitik, als ein US-amerikanisches Bundesgericht im Rechtsstreit zwischen dem Bundesstaat Ohio und dem US-Innenministerium *(State of Ohio v. United States Department of the Interior)* den Einsatz dieser Methode verlangte. Durch das Urteil wurde das Innenministerium dazu verpflichtet, Umweltschäden zukünftig auf Basis der Sanierungskosten zu berechnen und damit den sogenannten *non-use values* den Vorzug gegenüber den *use values* zu geben. Das Bundesgericht wies das Ministerium ferner an, zur Ermittlung der *existence values* die CVM zu verwenden, deren Verwendung von den Richtern befürwortet wurde.

Im gleichen Jahr ereignete sich im Prince-William-Sund vor Süd-Alaska eine der größten Umweltkatastrophen der Seefahrt, wodurch die Diskussion um die *Contingent Valuation* neuen Zündstoff erhielt. Aus der auf das Bligh-Riff aufgelaufenen *Exxon Valdez* waren 40.000 Tonnen Rohöl ausgelaufen, so

[11] ***C****omprehensive* ***E****nvironmental* ***R****esponse,* ***C****ompensation, and* ***L****iability* ***A****ct (CERCLA, 42 U.S.C. §§ 9601-9675).*

dass der US-Kongress als Reaktion auf die Ölpest mit dem *„Oil Pollution Act“* ein Gesetz verabschiedete, das als Grundlage für die Schadensfestsetzung und -regulierung zukünftiger Ölverschmutzungen dienen sollte.[12] Durch das Gesetz wurde die *National Oceanic and Atmospheric Administration (NOAA)* als Vertreter des Handelsministeriums beauftragt, die Richtlinien für diesen Regulierungsprozess festzulegen. Dabei standen den Forderungen der Umweltschützer nach der Einbeziehung der *non-use values* die Zweifel der Ölfirmen an der Tragfähigkeit der CVM entgegen.

Durch den Widerstand der Ölgesellschaften sah sich der Chefsyndikus der NOAA, T. Campbell, genötigt, eine Kommission zu gründen zur Schlichtung des Streitpunkts, ob die *Contingent Valuation* ein zuverlässiges und somit angemessenes Mittel sei. Als Vorsitzende des Gremiums setzte er mit K. Arrow und R. Solow zwei Nobelpreisträger für Wirtschaftswissenschaften ein und vervollständigte den Ausschuss mit E. Leamer, P. Portney, R. Radner und H. Schuman.[13] Ihr Ziel sollte die Begutachtung der Frage nach der Eignung der CVM zur Abschätzung verloren gegangener *existence values* und damit eine Bewertung als Grundlage für Schadensersatzforderungen sein. Als Endresultat ihrer Arbeit gab die Kommission bekannt, die CVM führe zu Schätzungen, die als Basis zur Bewertung von Schadensersatz verlässlich genug für die Verwendung vor Gericht seien.

Aus dem Gutachten zitierte Portney (1994, S. 8) die Grundaussage *„. . . the Panel concludes that CV studies [applications of the contingent valuation method] can produce estimates reliable enough to be the starting point of a judical process of damage assessment, including lost passive-use values“* und schlussfolgerte, diese Entscheidung habe dazu geführt, dass sich die Befürworter in Politik und Wissenschaft in ihrer bisherigen auf die CVM ausgerichteten Arbeit bestätigt fühlten. Tatsächlich erfreut sich das Verfahren seither einer weitgehenden Akzeptanz und wird inzwischen laut M. Cropper und A. Alberini (1998) neben der US-amerikanischen auch in der europäischen Umweltpolitik vermehrt eingesetzt.

[12] Die Ölreste in dem 2.000 km langen Küstengebiet sind bis heute nicht komplett abgebaut.

[13] Der Soziologieprofessor Schuman ist nach Portneys Aussage Experte für Umfrageforschung und war der einzige Nicht-Ökonom der Kommission.

3.2.2 Beschreibung der Methodologie

Nach Portney (1994, S. 7) gibt es keine standardisierte Vorgehensweise für das Design einer CV-Studie, dennoch bestehen beinahe alle Anwendungen aus drei Teilen:

Zuerst muss ein klar verständliches und möglichst detailliertes Szenario geschaffen werden, ein (hypothetisches oder tatsächlich geplantes) Programm oder politisches Konzept, zu welchem der Proband Stellung beziehen oder welches er bewerten soll. Als beispielhaftes Umweltszenario schlug Portney unter Anderem ein Programm zur Reduzierung der Luftverschmutzung vor, durch dessen Durchführung die jährliche Sterbewahrscheinlichkeit um einen bestimmten Wert gesenkt würde. Insgesamt soll dem Probanden ein klares Bild dessen gegeben werden, was er im Rahmen der Studie bewerten soll.

Weiterhin muss die Erhebung einen Mechanismus zur Verfügung stellen, durch welchen der Proband einen gewählten Wert oder eine getroffene Entscheidung kundtun muss. Diese Mechanismen sind vielfältig, einschließlich offener, also *„open ended“ (OE)* Fragen („Was ist der maximale Betrag, den Sie für ... bereit wären zu bezahlen?“), Gebote („Würden Sie $ 5 für dieses Programm zahlen? Ja? Würden Sie $ 10 zahlen? Wie wäre es mit ...“) oder Referenda („Die Regierung erwägt Programm X. Ihre jährliche steuerliche Belastung würde um Y ansteigen, wenn dies passiert. Wie würden Sie wählen?“)

Zu guter Letzt erheben CV-Studien üblicherweise Informationen zu sozioökonomischen Merkmalen der Teilnehmer (u. a. Alter, Geschlecht, Einkommen), ebenso wie für das spezifische Szenario relevante Eigenschaften wie die Einstellung zur Umwelt oder das Freizeitverhalten. Diese Variablen ermöglichen bei der Auswertung die Schätzung einer Zahlungsbereitschaftsfunktion, welche diese Charakteristika als mögliche erklärenden Variablen beinhaltet. Des Weiteren kann mit Hilfe von Kontrollfragen festgestellt werden, ob der Antwortende die Aufgabe verstanden hat und die Fragen ernsthaft beantwortet wurden.

Eine umfangreichere, vollständige Beschreibung der Elemente der *Contingent Valuation* Methode findet sich bei R. Mitchell und R. Carson (1989).

3.2.3 Diskussion der CVM

Der Artikel *„The Contingent Valuation Debate: Why Economists Should Care“* von Paul R. Portney diente 1994 im *Journal of Economic Perspectives* als Einleitung zur Diskussion der *Contingent Valuation* Methode. Während W. Michael Hanemann zunächst mit *„Valuing the Environment Through Contingent Valuation“* die Verwendung des Bewertungsverfahrens befürwortete, bezogen Peter A. Diamond und Jerry A. Hausman (1994) im Anschluss Stellung gegen die Einsetzbarkeit der Methode.

Diamond und Hausman (1994) kritisierten mit *„Contingent Valuation: Is Some Number Better than No Number?“* die Schwächen des Verfahrens mit der provokanten Frage, ob „irgendeine Zahl besser sei als [gar] keine“, da sie am Sinn der CVM zur Bewertung öffentlicher Güter zweifelten. Bereits zum Ende der Einleitung begründeten Diamond und Hausman (1994, S. 46) ihre Kritik an der Methode:

„In short, we think that the evidence supports the conclusion that to date, contingent valuation surveys do not measure the preferences they attempt to measure. Moreover, we present reasons for thinking that changes in survey methods are not likely to change this conclusion. Viewed alternatively as opinion polls on possible government actions, we think that these surveys do not have much information to contribute to informed policy-making. Thus, we conclude that reliance on contingent valuation surveys in either damage assessments or in government decision making is basically misguided.“

Die Fähigkeit, wirklich ökonomische Werte zu messen, wurde der *Contingent Valuation* hier von den Autoren abgesprochen, ferner sei eine qualitative Verbesserung der Aussagekraft der *Contingent Valuation* durch Veränderung bzw. Verfeinerung der Erhebungsmethoden nicht zu erwarten. Schlussendlich bezeichneten sie die Zuverlässigkeit der Methode als unzureichend für die Errechnung von Schadensersatzsummen. Die hauptsächliche Verantwortung für diese harsche Kritik an der CVM trage dabei nach Ansicht von Diamond und Hausman das sogenannte *„embedding“*.

Embedding

Im Jahr 1992 wurde der *„embedding effect“* von D. Kahneman und J. Knetsch erstmals einer systematischen Analyse unterzogen. Dabei rührt die Bezeichnung *„embedding“* daher, dass ein bestimmtes Gut in ein sogenanntes „inklusiveres“ Gut „eingebettet“ wird und dadurch die Zahlungsbereitschaft für das einzelne Gut nur geringfügig von der für das inklusivere, also umfangreichere Gut differieren soll. Unter einem inklusiveren Gut A^* ist in diesem Zusammenhang ein Gut zu verstehen, welches ein zuvor definiertes Gut A quantitativ oder qualitativ beinhaltet. Dieses Phänomen wird in der Literatur auch häufig als *„scope effect“* oder wie bei den Beispielen von Carson und Mitchell als *„nesting effect“* bezeichnet. So sei nach Diamond und Hausman (1994, S. 46) in einer Umfrage die Zahlungsbereitschaft für die Säuberung eines Sees ungefähr so hoch gewesen wie jene für die Reinigung von fünf Seen, inklusive des zuerst gefragten.

Als ein in der Praxis durchgeführtes Beispiel führten Diamond und Hausman (1994, S. 52 f) eine Studie von W. Schulze et al. von 1993 an und kritisierten dabei, das *Embedding* tauche selbst in Studien erfahrener CV-Analytiker auf, welche sich dieses Problems bewusst seien. In der Erhebung wurden die Probanden nach ihrer Zahlungsbereitschaft zur teilweisen oder vollständigen Sanierung einer auf der *„National Priorities List“* aufgeführten Sondermülldeponie in Montana befragt. Nachdem die Daten von Protestantworten, also von Nullen und von sehr hohen Zahlungsbereitschaften, bereinigt worden waren, belief sich die durchschnittlich geäußerte Zahlungsbereitschaft für die komplette Säuberung des Areals auf $ 72,46 (StdAbw $ 4,71), während hingegen für eine deutlich geringer ausfallende Teilsanierung durchschnittlich $ 72,02 (StdAbw $ 5,10) angegeben wurden.

Im zweiten Teil der Erhebung wurden nun die Probanden gefragt, ob sich ihre Antworten nur auf die besagte Deponie bezogen hätten oder teilweise auch die Sanierung anderer Deponien eingeschlossen hätten, oder ob es sich vielmehr um eine Art generelle Spendenbereitschaft für Umweltschutz gehandelt habe. Lediglich 16,9 % der Teilnehmer sagten aus, ihre Angaben bezögen sich nur auf die besagte Sanierung, was nach Meinung von Diamond und Hausman darauf schließen lasse, dass die Mehrheit der Befragten

selbst den Embedding-Effekt in ihren Antworten erkannt habe. Diese Teilnehmer wurden nun danach gefragt, welcher Anteil ihrer geäußerten Zahlungsbereitschaft sich auf das konkrete Sanierungsprojekt bezogen habe, um ihre Angaben anhand dieser Prozentangaben korrigieren zu können. Nach der Anpassung der Ergebnisse betrug die geäußerte *Willingness to pay* für die komplette Reinigung durchschnittlich noch $ 40,00 (StdAbw $ 2,62), während sich die Zahlungsbereitschaft für die Teilsanierung auf $ 37,15 (StdAbw $ 2,71) belief.

Diamond und Hausman (1994, S. 52 f) schlussfolgerten, dass diese Ergebnisse und insbesondere die hohe Zahl jener Teilnehmer, die selbst dieses Phänomen des „Einbettens“ erkannt hätten, ihre Hypothese zur eingeschränkten Einsetzbarkeit der *Contingent Valuation* Methode unterstützten. Unter Bezug auf Diamond et al. (1993) kritisierten sie dabei besonders, die Autoren hätten bei ihrer Studie keinen sogenannten *„Adding-up Test“* durchgeführt und könnten somit nicht einmal die Differenz dieser Ergebnisse erklären, die nicht allein auf Einkommenseffekten beruhen könnten.

Bei einem solchen *Adding-up Test* soll Gruppe 1 das öffentliche Gut X bewerten, Gruppe 2 hat das Gut X zur Verfügung und soll das Gut Y bewerten, Gruppe 3 soll die Güter X und Y (zusammen) bewerten. Nun sollte die gemeinsame Zahlungsbereitschaft für X + Y der Summe der beiden anderen Zahlungsbereitschaften entsprechen, abgesehen von einem (geringen) Einkommenseffekt. Schlussendlich bemängelten Diamond und Hausman (1994, S. 53), das Problem werde demnach auch von den Befürwortern der CVM nicht adäquat gelöst.

R. Carson und R. Mitchell (1995) schlüsselten den Begriff Embedding noch weiter auf, indem sie zwischen *„quantitative nesting“* und *„categorical nesting“* unterschieden und hierfür ein Gut B als eine Teilmenge von Gut A annahmen.[14] Demnach sei unter *quantitativem Nesting* zu verstehen, dass Gut Q auf einer gemeinsamen Skala messbar größer sei als Gut R, währenddessen bei *kategorischem Nesting* die Menge K aus den nichtleeren Mengen L und L* mit leerer Schnittmenge zusammengesetzt sei.

[14] Zur besseren Veranschaulichung der Beispiele von Carson und Mitchell werden im Folgenden die Buchstaben zur Bezeichnung der Güter nicht zitiert, sondern die Güter mit neuen Buchstaben versehen.

Als Beispiel für den ersten Fall könne gemäß Carson und Mitchell Gut Q 20 Tage bessere Sicht bedeuten und Gut R verbesserte Sicht an 6 dieser 20 Tage, im zweiten Fall wäre Gut K 20 Tage bessere Sicht *und* die Verbesserung der Wasserqualität, während L 20 Tage bessere Sicht und L* 20 Tage bessere Wasserqualität bedeuteten. Die Autoren räumten dabei ein, dass beide Arten von Nesting bzw. Embedding durch einander substituiert werden könnten, so sei im ersten Fall ziemlich offensichtlich R* 14 Tage verbesserte Sicht. Auch die umgekehrte Richtung sei möglich, da sich letzten Endes alles auf eine numerische Ebene herunterbrechen ließe und somit auch L und L* auf eine gemeinsame Skala projiziert werden könnten. Die Beispiele von Carson und Mitchell sind in den Tabellen 3.1 und 3.2 wiedergegeben.

Gut	**Effekt**	
Gut Q	bessere Sicht an 20 Tagen	$= R + R^*$
Gut R	bessere Sicht an 6 der 20 Tage	
Gut R*	bessere Sicht an 14 der 20 Tage	

Tabelle 3.1: Beispiel für quantitatives Embedding *(„quantitative nesting“)*

Gut	**Effekt**	
Gut K	20 Tage bessere Sicht und Wasserqualität	$= L + L^*$
Gut L	20 Tage bessere Sicht	
Gut L*	20 Tage bessere Wasserqualität	

Tabelle 3.2: Beispiel für kategorisches Embedding *(„categorial nesting“)*

Bei der von Diamond und Hausman kritisierten Studie von Schulze et al. (1993) finden beide Arten von Embedding Erwähnung, im Mittelpunkt der Diskussion steht dabei das kategorische Embedding, da nach den Zahlungsbereitschaften für die vollständige sowie die teilweise Sanierung einer Sondermülldeponie in Montana gefragt wird. Das quantitative Embedding kommt dann beim zweiten Schritt ins Spiel, als danach gefragt wird, ob diese Zahlungsbereitschaft auch andere Deponien eingeschlossen habe oder sich nur auf die Sanierung der besagten Deponie beziehe. Beim eingangs erwähnten

Beispiel mit der Reinigung der Seen handelt es sich ebenfalls um den quantitativen Fall von Embedding.

Der Effekt des Embedding kann also bei CVM-Studien immer dann auftreten, wenn seitens der Probanden die zu bewertende Maßnahme oder der zu erwartende Effekt einer solchen Maßnahme nicht klar von anderen Maßnahmen oder Effekten abgegrenzt wird bzw. werden kann. Im Blick auf die IT-Sicherheit könnte das beispielsweise bedeuten, dass ein Unternehmen eine Zahlungsbereitschaft für die Bekämpfung von 70 % der kursierenden Schadprogramme äußert, welche nur geringfügig über einer von ihm geäußerten Zahlungsbereitschaft für eine 30 %ige Reduzierung des Malware-Aufkommens liegt. Auch bei diesem Beispiel würde es sich um quantitatives Embedding handeln, bei welchem eine 70 %ige Verbesserung Gut Q entspräche, 30 % entsprächen Gut R und 40 % Gut R*.

Es ist daher wichtig, dass ein zu beurteilendes Szenario möglichst detailliert beschrieben wird, um durch die Präzision der Fragestellung die Gefahr von Missverständnissen zu minimieren und somit der Gefahr des Embedding entgegenwirken zu können. Nichtsdestotrotz ist es wichtig, dass bei einer Studie dem Auftreten von Embedding genug Aufmerksamkeit gewidmet wird und durch das Design der Befragung kontrolliert werden kann, ob der Effekt aufgetreten ist.

Sequencing

Das *„sequencing“* oder *„ordering problem“* kann laut Diamond und Hausman (1994, S. 49) auftreten, wenn im Rahmen einer Befragung mehrere Zahlungsbereitschaften geäußert werden sollen. Demnach könne die zweite *Willingness to pay* sowohl höher als auch niedriger ausfallen als die erste, wie eine Studie von K. Samples und J. Hollyer (1990) belege. In der Untersuchung wurden die in Tabelle 3.3 wiedergegebenen Zahlungsbereitschaften zum Schutz von Buckelwalen und Seehunden in unterschiedlicher Reihenfolge erfragt, mit dem Ergebnis, dass Wale an erster Stelle mit $ 125 und an zweiter mit $ 142 bewertet wurden. Bei den Seehunden hingegen fiel das Ergebnis umgekehrt aus, wurde zuerst nach ihnen gefragt, so wurden sie mit $ 103 bewertet, an zweiter Stelle jedoch nur noch mit $ 62.

	Zahlungsbereitschaft	
zu schützende Art	an 1. Stelle gefragt	an 2. Stelle gefragt
Buckelwale	$ 125	$ 142
Seehunde	$ 103	$ 62

Tabelle 3.3: Beispiel für Sequencing

Beide aufgetretenen Varianten des Sequencing wurden in der Arbeit von Diamond und Hausman (1994, S. 50) erläutert, dabei wurde zunächst die Erklärung für die höheren Werte der Wale von Samples und Hollyer (1990, S. 189) zitiert. So sei nach Meinung der Autoren die größere Beliebtheit der Buckelwale der Grund für die hohen Ergebnisse an zweiter Stelle, denn nach einer geäußerten Zahlungsbereitschaft für Seehunde hätten viele gezögert, bei Walen weniger großzügig zu sein, und dadurch die Werte in die Höhe getrieben. Dieses inflationäre Verhalten sei bei der anderen Version nicht aufgetreten, bei welcher die Frage zu Walen zuerst gestellt worden war. So war wohl nach Ansicht der Probanden nach der relativ hohen durchschnittlichen Zahlungsbereitschaft von bereits $ 103 für Seehunde eine erhebliche Steigerung auf $ 142 für den Schutz der Buckelwale nötig, woraus sich eine Differenz von $ 39 ergibt und ein Quotient von ca. $\frac{142}{103} \approx 1,4$. Dieser Unterschied fiel im umgekehrten Fall erheblich höher aus, so sank die Zahlungsbereitschaft von $ 125 für den Schutz der Buckelwale auf $ 62 für Seehunde, bei einer Differenz von $ 63 entspricht das ziemlich genau der doppelten Zahlungsbereitschaft. Ein weiterer möglicher Grund für dieses Verhalten könnte indes auch sein, dass der Schutz der Buckelwale von den Probanden generell mit höheren Kosten verbunden wurde als der Schutz der Seehunde, so dass sich die Differenz auch aus dieser Sichtweise begründen ließe.

Die sonst eher üblichen niedrigeren Werte bei der zweiten Frage, die im Beispiel auch bei den Seehunden aufgetreten waren, erklärten Diamond und Hausman (1994, S. 50) mit Einkommenseffekten. So sei nach der Bewertung der Wale, für die bereits „Geld ausgegeben“ wurde, weniger Einkommen übrig für die Seehunde an zweiter Stelle. Wäre nach dem Schutz einer dritten Tierart gefragt worden, so hätte es bei den unterschiedlichen Permutationen der Fragen nach der Zahlungsbereitschaften häufig Konstellationen gegeben, in

welchen die Zahlungsbereitschaften durch die spätere Position in der Reihenfolge der Fragen sukzessive gesunken wären. R. Carson et al. kommen 1998 in *„Sequencing and Valuing Public Goods“* zu dem Schluss, dass bei (perfekten) Substituten die Zahlungsbereitschaft bei der Permutation der Reihenfolge der Fragen für ein Gut von der ersten zur letzten Position (streng) monoton fallen müsse.

Bei der Erhebung der Zahlungsbereitschaft für IT-Sicherheit könnten in dem angedachten Szenario ebenfalls beide Formen des Sequencing auftreten, wenn die zwei gefragten Aspekte wie im Fall von Malware und Spam unterschiedliche Investitionsbereitschaft erwarten lassen. So kann davon ausgegangen werden, dass Unternehmen für den Schutz vor Schadprogrammen mehr bezahlen (wollen) als für den Schutz vor unerwünschten E-Mails, da die Folgen eines Malware-Vorfalls bei seinem Eintreten erhebliche Kosten verursachen können.

Wird den Unternehmen zunächst die Frage nach ihrer Zahlungsbereitschaft für die Senkung des Spam-Aufkommens präsentiert, so kann dies für die zu äußernde Zahlungsbereitschaft für die Reduzierung des Malware-Aufkommens zur Folge haben, dass eine entsprechende Steigerung gegenüber dem zuerst angegebenen Wert stattfindet. Es wäre daher anzunehmen, dass die zu Protokoll gegebenen Werte für den Schutz vor Malware an zweiter Stelle höher ausfielen als an erster Stelle. Schwer vorherzusehen ist hingegen der Einfluss, welchen die zuerst gestellte Frage nach der Zahlungsbereitschaft für den Schutz vor Schadprogrammen auf die geäußerten Werte für die Eindämmung der Spam-Problematik an zweiter Position haben könnte, da hier beide Formen von Sequencing im Bereich des Möglichen liegen. So könnte neben einem Einkommenseffekt, welcher die *Willingness to pay* hier senken würde, eine Art Sensibilisierung für Gefahren aus dem Internet stattfinden, so dass die geäußerten Werte für die Spam-Bekämpfung an zweiter Stelle höher ausfallen könnten als an erster Position.

Aus diesen Gründen ist es unerlässlich, bei der Erhebung von mehr als einer Zahlungsbereitschaft einen möglicherweise auftretenden Sequencing-Effekt in verschiedenen Versionen von Fragebögen zu kontrollieren, so dass Zusammenhänge zwischen den geäußerten Werten und der Reihenfolge der Fragen im Falle ihres Auftretens identifiziert werden können.

Weitere Kritikpunkte

King und Mazzotta (2000) wiesen darauf hin, dass Menschen zwar geübt seien im Umgang mit Marktgütern, so dass Kaufentscheidungen durchaus ihre individuelle Zahlungsbereitschaft wiedergäben, die *Contingent Valuation* setze aber implizit ein Verständnis für das zu bewertende Gut voraus, obwohl die meisten Menschen nicht in der (ökonomischen) Bewertung öffentlicher Güter geübt seien.

Weiterhin betonten King und Mazzotta die Wichtigkeit einer klaren Abgrenzung der von der Maßnahme zu erwartenden Effekte, welche es zu bewerten gelte. So verwiesen sie darauf, dass bei der Bewertung von Umweltgütern bei den Teilnehmern Assoziationen hervorgerufen werden könnten, welche für die Beantwortung der Frage nicht gewünscht seien. Beispielsweise könnten, wenn eigentlich nach der Zahlungsbereitschaft für bessere Sicht (durch die Reduzierung der Luftverschmutzung) gefragt werde, die Probanden ihre Angaben tatsächlich auf die Reduzierung des gesundheitlichen Risikos beziehen, welches sie mit der zu verringernden Luftverschmutzung in Verbindung brächten und somit ihre Antwort auf einen völlig anderen Sachverhalt basieren.

Im Zusammenhang mit Studien zum Umweltschutz sprachen Diamond und Hausman (1994, S. 52 f) bezüglich der geäußerten Zahlungsbereitschaften von einem *„warm glow (effect)“*. Bei diesem *„warm glow effect“* handelt es sich um eine Art „gönnerhaftes Gefühl“, mit dem Probanden ihre Besorgnis äußern und ihre Unterstützung für einen guten Zweck signalisieren möchten. D. King und M. Mazzotta (2000) merkten dazu an, dass Teilnehmer einer Studie teilweise nicht ihre ökonomische Einschätzung eines Gutes wiedergäben, sondern vielmehr versuchten, ihre Gefühle für das geschilderte Szenario in Zahlen zu fassen, und Bereitschaft zeigen wollten, für ein soziales Gut ihren Beitrag zu leisten. Dies geschehe selbst dann, wenn die Befragten das zu bewertende Gut eigentlich für sich selbst als unwichtig erachteten.

Diesen Eindruck belegten Diamond und Hausman (1994, S. 48) mit den Ergebnissen der Studie zum Schutz von Zugwasservögeln von D. Schkade und J. Payne (1993, 1994). In den verbalen Interviews wurden die Teilnehmer aufgefordert, bei ihren Entscheidungen „laut zu denken“, um den Interviewern

all ihre Gedankengänge mitzuteilen. Dabei brachten die Probanden sehr unterschiedliche Gedanken hervor, meistens wurden die Überlegungen mit der Aussage eingeleitet, es müsse etwas getan werden, bevor darüber nachgedacht wurde, welche Summe wohl angemessen sei. Ungefähr ein Sechstel der Teilnehmer stellte eine klare Verbindung zu wohltätigen Spenden her und basierte seine Angaben auf diesem Gedanken. Außerdem äußerte einer von fünf Befragten, er habe sich schlicht eine Zahl ausgedacht oder die Antwort geraten, jeder Vierte vertrat die Meinung, wenn jeder Einzelne seinen Teil dazu beitrage, müsse jeder Haushalt nicht so viel beitragen. Diese Faktoren führten Diamond und Hausman zu dem Schluss, dass seitens der Probanden wegen des hypothetischen Charakters der Fragestellung nicht die gleiche Ernsthaftigkeit an den Tag gelegt werde wie in realen Marktsituationen.

Im Übrigen merkte Hannes Spengler (2004, S. 152) an, dass im Rahmen von CV-Studien eine sonst in der Marketingforschung übliche Kalibrierung der Daten zur Befreiung von systematischen Verzerrungen nicht möglich sei und verwies auf Diamond und Hausman (1994, S. 54). Diese zählten Studien zu privaten Gütern und wohltätigen Spenden auf, in denen Kalibrierungsfaktoren zwischen 1,5 und 10 festgestellt worden waren und bemängelten, dass eine Übertragung auf öffentliche Güter aufgrund der ungewohnten ökonomischen Umstände nicht möglich sei. Sie betonten jedoch, dass in Ermangelung entsprechender Studien die Schlussfolgerung nicht zulässig sei, mit dem Kalibrierungsfaktor eins seien die besten Ergebnisse zu erzielen, und führten den argumentativ nicht widerlegten Vorschlag der NOAA an, als Standardwert für die Kalibrierung durch zwei zu dividieren.

Vorteile der CVM

In vielen Fällen ist die *Contingent Valuation* Methode die einzige Möglichkeit, ein (nicht marktfähiges) Gut ökonomisch zu bewerten. Dies trifft insbesondere auf Güter zu, für die keine Marktdaten zur Verfügung stehen oder für die es, wie im Fall der öffentlichen Güter, keine Märkte gibt.[15] Für King

[15]Spengler (2004, S. 149) stellte klar, dass sich zwar beispielsweise im Zusammenhang mit Staatsausgaben eine ökonomische Bewertung ableiten ließe, die Wertbestimmung hierbei jedoch nicht unbedingt mit den Vorlieben der Bevölkerung übereinstimmen müsse, sondern vielmehr die (persönlichen) Präferenzen der Entscheidungsträger wiedergebe.

und Mazzotta (2000) zeichnet sich die CVM darüber hinaus durch ihre Flexibilität aus, da mit ihr der Wert von nahezu Allem geschätzt werden könne. Es sei jedoch am Besten, Werte für Güter und Dienstleistungen zu schätzen, welche für den Befragten einfach zu identifizieren und klar zu verstehen seien und in getrennten Mengen betrachtet werden könnten, wie beispielsweise Tage der Erholung, selbst wenn kein beobachtbares Verhalten zur Verfügung stehe, diese Werte mit anderen Mitteln herzuleiten.

In seinem Artikel *„Valuing the Environment Through Contingent Valuation“* von 1994 verteidigte W. Michael Hanemann die CVM gegen die von Diamond und Hausman zusammengefasste Kritik und stellte klar, dass durch die Entdeckung und Beseitigung alter Schwächen enorme Fortschritte bei der Weiterentwicklung der *Contingent Valuation* Methode gemacht wurden. So habe schon Ciriacy-Wantrup (1947) erkannt, dass Befragungen nicht *per se* narrensicher seien und der Grad des Erfolgs vom Geschick bei Design und Implementation abhinge.

Die umfangreiche Nutzung sowie die großen Fortschritte der CVM bestätigten auch King und Mazzotta (2000) und begründeten diesen Erfolg unter Anderem mit der Verbesserung der Methodologie, welche die neueren Ergebnisse stichhaltiger und verlässlicher mache. Auch das bessere Verständnis für ihre Stärken und das Erkennen ihrer Grenzen sei mit ein Grund für die hohe Akzeptanz der Methode. Hanemann (1994, S. 21) berief sich auf R. Carson et al. (1994a), die in einem Übersichtsartikel mehr als 1.600 Studien und Publikationen aus über 40 Ländern erfasst hatten,[16] die sehr viele Themengebiete abdeckten, neben Umweltthemen unter Anderem auch das Verkehrs-, das Gesundheits- und das Bildungswesen. Des Weiteren gaben J. Hammit und J. Graham (1999, S. 58) zu bedenken, dass es trotz der weiterhin geführten Debatte über die *Contingent Valuation* wenige gute Alternativen zu dieser Methode gäbe.

Das Design ist für Hanemann (1994, S. 21 f) bei einer CV-Studie in allen Aspekten ausschlaggebend, sei es Stichprobenauswahl, Formulierung des Szenarios, Fragebogenstruktur oder die Datenanalyse, im Hinblick darauf fasst er die wichtigsten Punkte zur Gewährleistung der Verlässlichkeit zusammen.

[16] Carson (2000) verwies sogar auf über 2.000 Artikel und Studien von Regierungsbehörden und internationalen Organisationen in mehr als 50 Ländern.

So charakterisierten C. DiBona (1992) zufolge Kritiker wie der Präsident des *American Petroleum Institute* die *Contingent Valuation* mit dem Bild eines Interviewers, der im Supermarkt auf die Leute zugehe, sie kurz ihre Einkaufstaschen abstellen ließe und sie nach ihrer maximalen Zahlungsbereitschaft für einen Seeotter in Alaska oder ein Fleckchen Natur in Montana frage. Es erfordere keinen übermäßigen Scharfsinn, um zu erkennen, dass ein solcher Ansatz eher keine verlässlichen Resultate produziere und weder der Vorgehensweise guter CV-Forscher noch den Empfehlungen der NOAA-Kommission entspräche. Hanemann betonte daher, ernsthafte Befragungen vermieden im Allgemeinen das sogenannte *„convenience sampling“,* also beispielsweise das Anhalten potentieller Probanden auf der Straße.

Des Weiteren gestand Hanemann (1994, S. 22) ein, man gerate leicht in Versuchung, das zu bewertende Gut eher zu allgemein zu beschreiben mit Fragen wie „Was würden Sie für Umweltverträglichkeit bezahlen?“ und dadurch unklare Szenarien zu schaffen. Man könne keine Präferenzen für solche Abstraktionen messen, sondern müsse das Szenario präzisieren und die Probanden mit etwas Konkretem konfrontieren. Auch dürfe man im Zusammenhang mit der Ölkatastrophe keine hypothetische Frage stellen, welche die Havarie der *Exxon Valdez* rückwirkend ungeschehen machen solle, sondern müsse die Zahlungsbereitschaft für Maßnahmen erfragen, die bei einer zukünftigen Wiederholung den Schaden begrenzten.

Um den Embedding-Effekt in den Griff zu bekommen, riet Hanemann (1994, S. 34) zur Kontrolle mit einem *„Split-sample scope Test“.* Viele Studien hätten dies mit Erfolg getan, darunter auch eine Meta-Studie von Walsh et al. (1992) mit über 100 CV-Studien. Er führt weiter aus, Carson (1994) habe bei der Überprüfung von 27 Studien mit diesem Testverfahren in 25 Fällen eine signifikante Veränderung der Zahlungsbereitschaft für andere Mengen des zu bewertenden Gutes entdeckt. Hanemann monierte, dass Gegner der *Contingent Valuation* ihre Kritik jedoch gerade auf diese beiden Studien stützten, und erläuterte die Schwächen der zwei Erhebungen und wie diese zu den angreifbaren Fehlern geführt hätten.

Die von Diamond und Hausman (1994, S. 53) geäußerten Bedenken, eine Zahlungsbereitschaft könne auf einem *„warm glow“* basieren, zerstreute Hanemann (1994, S. 33) in einer Fußnote, „er kenne keine empirischen Beweise,

dass Menschen ein gönnerhaftes Gefühl bekämen, wenn es um eine Zustimmung zur Erhöhung ihrer Steuerlast ginge, sei es im realen Leben oder in einer CV-Studie". Weiterhin zitierte er G. Becker (1993) mit der Aussage: *„[I]ndividuals maximize welfare as they conceive it, whether they be selfish, altruistic, loyal, spiteful or masochistic."*

Auch der Forderung von Diamond und Hausman nach Expertenentscheidungen, die ihrer Ansicht nach sinnvoller seien als das Heranziehen der CVM, erteilte Hanemann (1994, S. 38) eine Absage, da nach seiner Meinung in vielen Fällen die relevanten Experten die Bevölkerung selbst sei. Zwar sollten Experten eine führende Rolle bei der Feststellung der physischen Schäden spielen und bei Berechnung der Reinigungs- und Wiederherstellungskosten, es sei aber unklar, wie unbeschädigter Natur ein Wert beigemessen werden könne, und somit sei das Aufgabe der Bevölkerung.

Obwohl das Verfahren der *Contingent Valuation* wie bereits gesehen ein gut durchdachtes Fragebogendesign benötigt, sind nach Ansicht von King und Mazzotta (2000) weder CV-Studien selbst noch ihre Ergebnisse schwer zu beschreiben und zu analysieren. Konkrete Geldbeträge könnten demnach als Mittelwert oder Median pro Einwohner oder Haushalt betrachtet werden oder zu einem Gesamtwert für die betroffene Bevölkerung(sgruppe) aggregiert werden. Spengler (2004, S. 149) stellte im Zusammenhang mit der Schätzung des Wertes eines Statistischen Lebens eine beispielhafte Rechnung auf: Ergäbe eine repräsentative Umfrage für ein Programm zur zehnprozentigen jährlichen Reduzierung von Tötungsdelikten eine durchschnittliche Zahlungsbereitschaft von 25 Euro pro Haushalt, so führe dies bei ca. 40 Mio. Haushalten und 2.500 jährlichen Delikten zu einer impliziten Bewertung eines (vermiedenen) Delikts von $(\frac{40\text{Mio.}\times 25\text{Euro}}{0{,}1\times 2.500}) = 4$ Mio. Euro.

Zur Zuverlässigkeit der Resultate fassten King und Mazzotta (2000) zusammen, dass *Contingent Valuation* das am weitesten anerkannte Verfahren zur Schätzung eines ökonomischen Gesamtwertes sei, inklusive *non-use* oder *passive use values,* und diese könnten damit ebenso geschätzt werden wie *use values.* Dabei könnten *use* und *non-use values* nach Hanemann (1994, S. 20) mit der CVM im Gegensatz zu anderen Verfahren auch getrennt gemessen werden. Hanemann (1994, S. 29) unterstrich die hohe Qualität der Ergebnisse

bei *use values,* die Carson et al. (1994b) bei über 80 Studien entdeckt hatten, und verwies beispielhaft auf eine Differenz von drei Prozent in einem ersten Test von J. Knetsch und R. Davis (1966) zwischen der *Contingent Valuation* Methode und dem Reisekostenansatz.

Portney (1994, S. 16) schloss seine Ausführungen mit der Aussage, es erscheine ihm unumgänglich, dass die CVM in der öffentlichen Politik eine Rolle spielen werde, da sowohl Aufsichtsbehörden als auch staatliche Ämter, welche für die Schadensabschätzung bei natürlichen Ressourcen verantwortlich seien, bei ihrer Arbeit zunehmend von ihr Gebrauch machten.

Dass die *Contingent Valuation* Methode bis heute eine wichtige Rolle in der Feststellung der Höhe von Schadensersatz spielt, zeigt sich an den Urteilen zum Tankerunglück in Alaska. Im Fall der *Exxon Valdez* errechneten R. Carson et al. (1992) aus dem korrigierten Median der Zahlungsbereitschaften einen Schaden von 4,4 Mrd. Dollar und erachteten diesen Wert als untere Schranke der verursachten Kosten. Dabei beliefen sich laut Greenpeace (2005) allein die Kosten für die nicht vollständig mögliche Säuberung des Küstenabschnitts auf über 2 Mrd. Dollar. Folglich wurde die Ölgesellschaft 1994 in erster Instanz zu einer Strafe von 5 Mrd. Dollar verurteilt, ein Berufungsgericht setzte 2001 das Strafmaß auf eine Zahlung von 4,5 Mrd. Dollar fest.

3.2.4 CVM in der Kriminometrie

Während sich die *Contingent Valuation* neben ihrem Anwendungsschwerpunkt in der Ressourcen- und Umweltökonomik auch schon in einigen anderen Bereichen der Nationalökonomie etabliert hat, kommt sie in der empirischen Kriminalitätsforschung bisher kaum zum Einsatz. Sowohl der Artikel von J. Ludwig und P. Cook (2001) als auch die Arbeit von M. Cohen, R. Rust, S. Steen und S. Tidd (2004) fokussierten dabei auf die Kosten von Gewaltkriminalität und ermöglichten durch ihre Ergebnisse Rückschlüsse auf den Wert eines verhinderten Tötungsdeliktes[17] und somit implizit den Wert eines Statistischen Lebens.

[17] Streng genommen hatten Ludwig und Cook nach der Vermeidung von Schussverletzungen gefragt.

Ludwig und Cook (2001, S. 212 f) interviewten im Rahmen einer Telefonbefragung des *1998 National Gun Policy Survey (NGPS)* 1.204 amerikanische Erwachsene als Vertreter eines Haushalts in einer Reihe von Fragen zu ihrer Einstellung zu Regierung und aktuellen oder vorgeschlagenen Waffengesetzen, bevor sie zur Kernfrage der Befragung kamen:

„Suppose that you were asked to vote for or against a new program in your state to reduce gun thefts and illegal gun dealers. This program would make it more difficult for criminals and delinquents to obtain guns. It would reduce gun injuries by about 30 %, but taxes would have to be increased to pay for it. If it would cost you an extra [$ 50 / $ 100 / $ 200] in annual taxes would you vote for or against this new program?“

Die Frage nach der Zahlungsbereitschaft für eine Reduzierung von Gewaltverbrechen unter Einsatz von Schusswaffen wurde als Referendum gestellt, wie es vom NOAA-Gremium von K. Arrow et al. (1993) vorgegeben wird, der Betrag der Steuererhöhung wurde dabei zufällig von der Befragungssoftware bestimmt. Als Folgefrage sollten die Probanden abhängig von der Antwort auf die erste Frage äußern, ob sie (im Falle der Zustimmung) zur Zahlung des doppelten bzw. (bei Ablehnung) zur Zahlung des halben Wertes bereit wären, die Zahlungsbereitschaften lagen in diesem Szenario also zwischen $ 25 und $ 400.

Da laut Ludwig und Cook (2001, S. 214 ff) die nicht-parametrische Schätzung nicht zwischen den Gebotswerten interpoliere und keine Extrapolation über das Höchstgebot von $ 400 zulasse, regressierten sie unter neuen Annahmen über die einzelnen Intervalle. Auf Basis des neuen Modells wurde nun die durchschnittliche Zahlungsbereitschaft pro Haushalt sowie pro vermiedenem Gewaltdelikt mit Schusswaffen errechnet, aus diesen Ergebnissen erfolgte dann die Ermittlung des Werts einer vermiedenen Schussverletzung mit Todesfolge über den Anteil tödlicher Delikte.

Cohen et al. (2004, S. 7) beschränkten sich bei ihrer Studie zur Zahlungsbereitschaft für *„Crime Control Programs“* nicht wie Ludwig und Cook auf Gewaltverbrechen mit Schusswaffeneinsatz, sondern zogen vielmehr verschiedene Straftaten heran, für deren Vermeidung sie die *Willingness to pay* ermitteln wollten. Dabei wurden für jeden Teilnehmer der Studie zufällig drei

von fünf Verbrechen ausgewählt, namentlich Einbruchdiebstahl, schwere bzw. gefährliche Körperverletzung, bewaffneter Raub, Vergewaltigung bzw. sexuelle Nötigung sowie Mord, und in zufälliger Reihenfolge vorgegeben, zu denen sie sich dann äußern sollten. Die Autoren gaben als Begründung für die Auswahl der Delikte an, diese seien die am einfachsten zu verstehenden wichtigen Straftaten. Den Probanden seien aber keine Definition gegeben worden oder nähere Informationen zur Opferwahrscheinlichkeit oder der durchschnittlichen Schwere der Verletzungen bei den Gewaltverbrechen. An der repräsentativen Umfrage, welche wie die zuvor präsentierte Erhebung im Referendumsformat ablief, nahmen 1.300 US-Bürger teil, Cohen et al. (2004, S. 6) unterstrichen dabei, sie haben auch sonst den Empfehlungen von Arrow et al. (1993) in nahezu allen Punkten entsprochen.

Bemerkenswert ist der ausdrückliche Hinweis für die Teilnehmer in der Einleitung zum WTP-Abschnitt, dass es sich bei den geäußerten Zahlungsbereitschaften um Geld handle, welches ihnen dann nicht mehr für Essen und andere notwendige Alltagsausgaben zur Verfügung stehe. Zudem träfe der Proband bei der Abstimmung nicht nur eine Entscheidung für seinen eigenen Haushalt, sondern gleichwohl für jeden Haushalt in dessen *„community“*. Dabei wurde die Wahl des mehrdeutigen Begriffs in einer Fußnote erläutert, da sich diesen jeder Teilnehmer selbst spezifizieren sollte, um zu erlauben, eine eigene Auswahl von Menschen in die (Kosten- und Nutzen-) Effekte einzuschließen.

Die zentrale Frage zur ersten Deliktsart formulierten Cohen et al. (2004, S. 7) wie folgt:

„Last year, a new crime prevention program supported by your community successfully prevented one in every ten [INSERT CRIME] from occuring in your community. Would you be willing to pay [INSERT AMOUNT] per year to continue this program?“

Dabei variierten die in den Text eingefügten zufälligen Zahlenwerte zwischen $ 25 und $ 225 in Schritten von $ 25. Im zweiten Teilschritt wurde dann die Frage wiederholt, wobei bei Zustimmung in der ersten Frage der Betrag um $ 25 erhöht, bei Ablehnung um $ 25 gesenkt wurde. Wurden $ 25 in der ersten Frage abgelehnt, reduzierte sich der zweite Wert auf $ 10. Hernach

wurden die Teilnehmer um eine kurze Begründung für ihre Antwort gebeten.

Bei den folgenden Delikten wurden die Probanden explizit gebeten, das vorangegangene Szenario außer Acht zu lassen, dann erfolgte eine analoge Schilderung der zweiten bzw. dritten Verbrechensart. Begründet wurde diese Instruktion mit der Annahme, dass ein Befragter zwar beispielsweise zur individuellen Zahlung von jeweils $ 200 zur Verhinderung von Mord und von Körperverletzung bereit wäre, nicht aber zu aggregierten $ 400 zur Vermeidung beider Delikte. Zum Schluss wurde zur Kontrolle von Einkommenseffekten gefragt, ob die Teilnehmer auch bereit wären, die Summe ihrer Angaben für die Reduzierung aller genannter Deliktsarten *„out of [their] own pocket“* zu bezahlen.

Cohen et al. (2004, S. 13 f) ermittelten dann mit der beispielhaft auf Seite 69 vorgestellten Vorgehensweise den impliziten Wert eines verhinderten Delikts für jede der betrachteten Kriminalitätskategorien. Cohen et al. (2004, S. 27 f) stellten zudem fest, dass diese Werte zwischen 2-3 Mal höher für (schwere) Körperverletzung, Vergewaltigung sowie Mord und 5-10 Mal höher für Raub und Einbruchdiebstahl waren als in vorangegangenen Schätzungen. Die Autoren argumentierten, dass ihre eigenen Resultate aus früheren Opferkostenstudien D. Nagin (2001a, 2001b) zufolge auf den Kosten für ein Individuum unter Außerachtlassung externer sozialer Kosten basierten, die *Contingent Valuation* Methode jedoch eine vollständigere Bewertung der gesellschaftlichen Kosten von Kriminalität erlaube.

Hervorzuheben ist bei der Studie von Cohen et al. (2004, S. 7) im Übrigen die Idee, den Probanden als hypothetisches Szenario ein bereits erfolgreich durchgeführtes Programm der Regierung mit *ex post* messbarem Erfolg zu präsentieren, um dessen (fiktive) Fortführung es gehe. Damit wird das Szenario für den Zuhörer weniger abstrakt und verliert etwas seinen hypothetischen Charakter, wodurch ernsthaftere Reaktionen erwartet werden können als bei der Äußerung von Zahlungsbereitschaften für eher abstrakte und daher wenig greifbare Szenarien.

Die beiden Umfragen zu Kosten von (Gewalt-)Kriminalität erfüllen einen Großteil der vom NOAA-Panel festgelegten Anforderungen für *Contingent Valuation* Studien. Dennoch müssen die zwei Erhebungen in einem entscheidenden Punkt kritisiert werden, denn trotz der sorgfältigen Vorbereitung und

der korrekten Durchführung der beiden Studien ist ihnen gemein, dass der Embedding-Effekt nicht ausreichend berücksichtigt wurde. Spengler (2004, S. 158) weist in diesem Zusammenhang auf die unterschiedlichen Werte für ein vermiedenes Tötungsdelikt von Ludwig und Cook (2001) zwischen $ 4,2 Mio. und $ 6,5 Mio. sowie Cohen et al. (2004) von $ 9,9 Mio. hin und argumentiert mit dem unterschiedlichen Rückgang um 30 % bzw. um 10 %. Sein Einwand ist dabei *per se* richtig, jedoch sollte beachtet werden, dass der Wert von Ludwig und Cook (2001, S. 221) aus den Umfrageergebnissen hergeleitet wurde, obwohl nach eigenen Angaben bei der Fragestellung auf die Letalität einer Schussverletzung nicht explizit eingegangen worden war. Da auch ein Vergleich mit den anderen von Cohen et al. angeführten Straftatkategorien wie beispielsweise (bewaffnetem) Raub sehr schwierig ist, sollte von einem numerischen Vergleich der Ergebnisse aufgrund der unterschiedlichen inhaltlichen Schwerpunkte der WTP-Fragen abgesehen werden.

Trotz der unzureichenden Behandlung der Embedding-Problematik sind die Untersuchungen von Ludwig und Cook (2001) und Cohen et al. (2004) die entscheidenden Studien im Bereich der Kriminometrie und ein sehr gutes Beispiel für die Umsetzung der *Contingent Valuation* bei der Schätzung von Kriminalitätskosten, die thematisch nicht auf Gewaltkriminalität begrenzt bleiben müssen. Darüber hinaus gibt es noch weitere CVM-Studien aus dem Umfeld der Kriminalitätsforschung, wie beispielsweise von G. Zarkin et al. (2000) zur Kostenquantifizierung der Behandlung von Drogenmissbrauch, die hier allerdings keinen Eingang finden.

Spengler (2004, S. 157) fasst zusammen, die *Contingent Valuation* Methode könnte gerade im Bereich der Kriminalpolitik eine wichtige Entscheidungshilfe für erwogene Präventionsstrategien sein und plädiert für eine häufigere Anwendung des Bewertungsverfahrens in der Zukunft. Kriminalität stelle für die meisten Bürger im Gegensatz zu manchen relativ abstrakten Problemstellungen ein klar fassbares und teilweise selbst erlebtes Szenario dar, für dessen Bekämpfung Präferenzen bestünden und somit über die Zahlungsbereitschaft die Kosten von Kriminalität verhältnismäßig einfach quantifizierbar machten.

Zusammenfassend kann festgehalten werden, dass die *Contingent Valuation* Methode in vielen Fällen die einzige Möglichkeit zur Bewertung eines

Gutes ist, besonders wenn wie im Falle öffentlicher Güter eine anderweitige Erhebung eines (realen) Marktwertes nicht möglich ist. Der Einsatz und die Umsetzung der CVM erweist sich dabei als recht unproblematisch, wenn die Vorgaben von Portney (1994) und Hanemann (1994) unter Einbeziehung der Empfehlungen der NOAA-Kommission beachtet werden. Auch können Abweichungen von den Vorschlägen des Gremiums durchaus argumentativ begründet werden, die wichtigsten Fehlerquellen, die Diamond und Hausman (1994) als Gründe gegen den Einsatz der Methode vorbringen, erfordern jedoch besondere Aufmerksamkeit.

Nachdem Hanemann (1994) dem Argument von Diamond und Hausman (1994) widersprochen hat, geäußerte Zahlungsbereitschaften beruhten auf einem *„warm glow“* und somit nur auf einem gönnerhaften Gefühl anstatt auf ökonomischen Gesichtspunkten, sollte das Problem des Embedding im Mittelpunkt der Aufmerksamkeit beim Design einer CV-Erhebung stehen. Auch sollte die Gefahr des Sequencing bei der Ausarbeitung einer *Contingent Valuation* Studie beachtet werden, wenn mehr als eine *Willingness to pay* bekundet werden soll. Die vielseitigen Einsatzmöglichkeiten gaben letzten Endes auch den Ausschlag für die Entscheidung, bei der Schätzung der Kosten von Schadprogrammen und unerwünschten E-Mails die *Contingent Valuation* Methode unter Berücksichtigung gerade dieser Schwächen einzusetzen.

Hanemann (1994, S. 38) zog als Fazit, dass CV-Studien nicht unter allen Umständen einsetzbar seien und nicht immer ein plausibles Szenario aufbauen könnten, auch seien ihre Fragebögen nicht alle von hoher Qualität. So kam er zu dem Schluss, dass jede einzelne Studie eingehend geprüft werden müsse, dies gelte jedoch für jede empirische Studie.

3.3 Multivariate Analysemethoden

Nach der obligatorischen deskriptiven Analyse der Daten werden in Abschnitt 5.2 die Ergebnisse der Faktorenanalyse vorgestellt, im Anschluss folgen die Resultate mehrerer Regressionsanalysen in Abschnitt 5.3. Aus diesem Grund wird in diesem Abschnitt ein kurzer Einblick in die beiden Analyseverfahren gegeben.

3.3.1 Faktorenanalyse

Liegt für eine Regressionsanalyse nur eine kleine Zahl von erklärenden Variablen vor, so treten bei diesem Lösungsansatz nur selten Schwierigkeiten auf. Mit steigender Zahl der möglichen Einflussvariablen wächst jedoch die Wahrscheinlichkeit, dass die Variablen, mit denen die abhängige Variable erklärt werden soll, untereinander nicht unabhängig sind und Probleme bei der Interpretation der Ergebnisse hervorrufen. Aus diesem Grund sollte im Vorfeld einer Regression versucht werden, solche Abhängigkeiten, welche beispielsweise nicht bereits in einer Korrelationsmatrix aufgedeckt werden konnten, zu finden. Die im empirischen Kapitel dieser Arbeit eingesetzte Faktorenanalyse dient der Dimensionsreduktion und kann durch die Zusammenfassung ähnlicher Variablen zu als Faktoren bezeichneten latenten Variablen auf solche Abhängigkeiten hinweisen. Vornehmliches Ziel der Analyse soll also sein, eine beliebige Anzahl von Variablen durch eine (erheblich) kleinere Zahl von Faktoren zu erklären.

Nach der Auswahl der in die Analyse einzubeziehenden Variablen wird aus diesen die Korrelationsmatrix errechnet, so dass für K Variablen eine $K \times K$-Matrix entwickelt wird. Bei der Extraktion von $J \ll K$ Faktoren sollen die N Beobachtungen der Variablen mit durch sogenannte Faktorladungen a_{jk} gewichteten Faktoren erklärt werden, die mathematische Grundlage bildet das hier skizzenhaft erläuterte *Fundamentaltheorem der Faktorenanalyse.*

Die n-te Beobachtung der Variablen x_k wird dann wie folgt durch Faktoren erklärt:

$$x_{kn} = a_{1k}f_{1n} + a_{2k}f_{2n} + \ldots + a_{Jk}f_{Jn} = \sum_{j=1}^{J} a_{jk}f_{jn} \ . \tag{3.1}$$

Nach der Standardisierung der Beobachtungen ergibt sich die Matrixschreibweise

$$Z = FA^T \ , \tag{3.2}$$

die in der Literatur als *Grundgleichung der Faktorenanalyse* bekannt ist, dabei sei A^T die transponierte Faktorladungsmatrix. Die Korrelationsmatrix R ergibt sich daher aus der standardisierten Datenmatrix als

$$R = \frac{Z^T Z}{n-1} \overset{(3.2)}{=} \frac{AF^T F A^T}{n-1} \ . \tag{3.3}$$

Durch die Standardisierung der Beobachtungen gilt für die mit C bezeichnete Korrelationsmatrix der Faktoren

$$C = \frac{F^T F}{n-1} \ , \tag{3.4}$$

und unter der Annahme der Unkorreliertheit der Faktoren folgt mit

$$C = I \tag{3.5}$$

ihre durch die Einheitsmatrix I ausgedrückte lineare Unabhängigkeit bzw. Orthogonalität, so dass

$$R = A\frac{F^T F}{n-1}A^T \overset{(3.4)}{=} ACA^T \overset{(3.5)}{=} AA^T \tag{3.6}$$

gilt.

Dieser in Gleichung (3.6) dargestellte Zusammenhang zwischen der Korrelationsmatrix R und der Faktorladungsmatrix A wird als Fundamentaltheorem der Faktorenanalyse bezeichnet. In Worten ausgedrückt zeigt diese Herleitung, wie unter der Annahme linear unabhängiger Faktoren der Zusammenhang zwischen Korrelationsmatrix R und Faktorladungsmatrix A vereinfacht werden kann.

Die Variablen, die in eine Faktorenanalyse einfließen, können als Vektoren aufgefasst werden, die zueinander in bestimmten Winkeln stehen, welche sich wiederum über den Cosinus der Werte der Korrelationsmatrix berechnen lassen. Ein Korrelationskoeffizient von $r = 1$ impliziert somit einen Abweichungswinkel von 0°, orthogonale Vektoren entsprechen hingegen einer Korrelation von null, und die entgegengesetzte Ausrichtung von Variablen mit $r = -1$ ergibt einen Winkel von 180°. Ebenso sind die zu extrahierenden Faktoren als (orthogonale) Vektoren zu verstehen, welche als Basis einen Vektorraum aufspannen sollen, in dem alle ursprünglichen Variablen als Linearkombination dieser Basisvektoren dargestellt werden können.

Bei der sogenannten Hauptkomponentenanalyse ist das primäre Ziel, dass ein erster zu ermittelnder Faktor einen möglichst großen Teil der Gesamtvarianz erklärt, der zweite Faktor wiederum einen möglichst großen Teil der Restvarianz, und so weiter. Aus mathematischer Sicht entspricht diese Vorgehensweise der Suche nach den Eigenvektoren der Matrix, deren Eigenwerte λ_k

dann der Größe nach absteigend sortiert werden. Da der Eigenwert eines Faktors gleich der Summe seiner quadrierten Faktorladungen über alle Variablen ist, hat der Faktor mit dem höchsten Eigenwert den größten Erklärungsgehalt, gefolgt vom zweiten Faktor bis hin zum letzten. Das *charakteristische Polynom*

$$P_K(\lambda) = |A - \lambda I_K| \tag{3.7}$$

besitzt als Polynom K-ten Grades K nicht notwendigerweise disjunkte Nullstellen für die Eigenwerte λ_k, die dazugehörenden Eigenvektoren e_k sind dann die Lösungen des homogenen linearen Gleichungssystems

$$(A - \lambda_k I_K)e_k = 0 \ . \tag{3.8}$$

Werden im vorliegenden Beispiel jedoch K Faktoren extrahiert, so ist die gewünschte Dimensionsreduktion nicht erfolgt, sondern es wurden lediglich die Variablen mit einer Basis der Dimension K dargestellt. Zur Bestimmung der optimalen Anzahl der zu extrahierenden Faktoren gibt es mehrere Vorgehensweisen, von den die zwei wohl bekanntesten Vertreter kurz umrissen werden sollen:

Der objektivere der beiden Ansätze ist das *Kaiser-Kriterium*[18] und basiert auf dem Hintergrund, dass die Eigenwerte ein Indikator für die durch den jeweiligen Faktor erklärte Varianz der Beobachtungswerte sind. Somit erklären Faktoren mit hohen Eigenwerten einen relativ großen Anteil der Gesamtvarianz der Variablen. Das Kaiser-Kriterium besagt, dass nur jene Faktoren in der Analyse zu berücksichtigen sind, deren Eigenwerte größer als eins sind, da auf diese Weise sichergestellt wird, dass jeder Faktor einen größeren Erklärungsgehalt hat als eine einzelne Variable, deren Varianz aufgrund der Standardisierung gleich eins ist.

Beim *Scree-Test* hingegen ist eine so eindeutige Bestimmung nicht immer möglich, da hier mit dem sogenannten *Elbow* ein Knick im Verlauf einer Gerade zwischen den äquidistant angeordneten absteigenden Eigenwerten gefunden werden muss. Die Idee dieser Methode ist nun, nur die Faktoren links des Knicks zu berücksichtigen, da durch die große Differenz zum nächsten Eigenwert dessen zusätzliche Aussagekraft einen verhältnismäßig kleinen

[18] Das Kaiser-Guttman-Kriterium wird in der Literatur häufig nur als Kaiser-Kriterium bezeichnet.

Nutzen bringt, der Erklärungsgehalt der restlichen Eigenwerte wird als Scree, also Schutt oder Geröll bezeichnet. Da bei manchen Kurven durch ähnliche Differenzen kein Knick oder aufgrund größerer Sprünge in beispielsweise zwei Punkten mehr als ein Kandidat für jenen Ellenbogen zur Verfügung stehen, mutet dieser Ansatz durch seinen Interpretationsspielraum eher subjektiv an. Aus diesem Grund fiel die Entscheidung zugunsten des (eindeutigen) Kaiser-Kriteriums, bei dem zudem sichergestellt ist, dass der Erklärungsgehalt eines Faktors höher ist als der einer Variablen.

Analog zur Regressionsanalyse gibt es bei der Faktorenanalyse eine Restvarianz, da ein Teil der Varianz nicht durch die extrahierten Faktoren erklärt wird, jener Teil der Gesamtvarianz, welcher durch die Faktoren erklärt werden kann, wird als *Kommunalität* bezeichnet. Im Gegensatz zur in dieser Arbeit nicht eingesetzten *Hauptachsenanalyse,* bei welcher sich die Varianz jeder Variablen aus ihrer Kommunalität und ihrer Einzelrestvarianz zusammensetzt, wird bei der *Hauptkomponentenanalyse* unterstellt, die Varianz einer Variablen könne durch die extrahierten Faktoren vollständig erklärt werden. Die unterstellte Nichtexistenz dieser Einzelrestvarianzen stellt einen Informationsverlust dar, welcher aufgrund der Zielsetzung der Hauptkomponentenanalyse jedoch hingenommen werden kann. Bei dieser Analyse geht es nicht um die vollständige Erklärungen der Varianzen der Ausgangsvariablen, sondern um Zusammenhänge zwischen den Variablen, also eine Zusammenfassung durch die Faktoren und somit um eine reine Dimensionsreduktion.

Durch diese Annahme der Hauptkomponentenanalyse ergibt sich für die Summe aller Faktoren eine Kommunalität von eins, die Varianz einer Variablen wird also vollständig erklärt, wenn alle möglichen Faktoren extrahiert werden. Somit stellt bei der Auswahl einer kleineren Zahl von Faktoren anhand der oben vorgestellten Kriterien die Kommunalität einer Variablen ein Maß der Qualität des Erklärungsgehalts der ausgewählten Faktoren für die Variable dar. Je größer der Wert innerhalb des Intervalls $[0; 1]$ ist, desto besser wird die Varianz einer Variablen durch die extrahierten Faktoren erklärt, mit jedem zusätzlichen Faktor steigt die Kommunalität monoton bis zu ihrem Maximum von eins.

Nach der Bestimmung der optimalen Anzahl der Faktoren gilt es nun, die Ergebnisse zu interpretieren, bei der Hauptkomponentenanalyse also um die

Suche eines geeigneten Sammelbegriffs für jeden Faktor, sofern er nicht nur eine, sondern mehrere zusammenhängende Variablen abbildet. Hierfür werden die Faktorladungen der extrahierten Faktoren für die einbezogenen Variablen in einer *Faktorladungsmatrix* betrachtet. Dabei sind betragsmäßig hohe Faktorladungen von mindestens $\pm 0,5$ stets zu berücksichtigen, da diese damit immerhin zumindest 25 % der Varianz einer Variablen erklären, es liegt jedoch im Ermessen des Betrachters, ab welchem Grenzwert er Faktorladungen in der Analyse einbezieht. Die Summe der quadrierten Faktorladungen einer Variablen ergibt dabei ihre Kommunalität, demnach gilt für große Kommunalitäten, dass hier üblicherweise mindestens eine hohe Faktorladung $|a_{jk}| \geq 0,5$ vorliegt, dies ist jedoch nicht zwingend notwendig.

Zur einfacheren Interpretation erfolgt an dieser Stelle üblicherweise eine Rotation, durch welche das kartesische Koordinatensystem an die Ausrichtung der (orthogonalen) Faktoren angeglichen wird. Häufig kommt dabei die auch hier verwendete Varimax-Rotation zum Einsatz, bei welcher durch die optimale orthogonale Drehung die Summe der erklärenden *Vari*anzen der Faktorladungen *max*imiert wird. Bei der dann folgenden Interpretation der Faktoren sollte das Hauptaugenmerk auf den (betragsmäßig) hohen Faktorladungen unter Berücksichtigung der Vorzeichen liegen.

Ein regelmäßig bei Faktorenanalysen auftretendes Problem ist das sogenannte *Missing-Value-Problem,* also der Umgang mit fehlenden Angaben durch unvollständig beantwortete Fragebögen. Backhaus et al. (2006) geben zur Lösung dieses Problems verschiedene Optionen der von ihnen verwendeten Software SPSS an, die teilweise erheblich in die Resultate der Analyse eingreifen würden. Die im Rahmen dieser Arbeit eingesetzte Software Stata bietet diese automatisierten Möglichkeiten nicht, so dass im Falle des Auftretens von Missings ein manuelles Eingreifen des Benutzers nötig wäre.

Eine solche Korrektur der Datenbasis musste bei den in Kapitel 5 analysierten Antworten vorgenommen werden, da beispielsweise die vorgeschlagene Nichtberücksichtigung unvollständiger Fragebögen aufgrund ihrer immensen Anzahl nicht möglich war. Die Vorgehensweise zur Lösung dieses Problems wird im Zuge der Vorbereitung der Faktorenanalyse auf Seite 130 näher erläutert.

3.3.2 Regressionsanalyse

Da die lineare Regression sowohl im bivariaten als auch im multivariaten Fall nicht nur in der empirischen Wirtschaftsforschung, sondern auch beispielsweise in den Natur- oder Sozialwissenschaften zu den am häufigsten verwendeten Analysemethoden gehört, wird sie in dieser Arbeit als bekannt vorausgesetzt. Daher soll zum Abschluss dieses Kapitels nur eine Betrachtung der ebenfalls in dieser Arbeit eingesetzten logistischen Regression sowie der schrittweisen Regression vorgenommen werden.

Zuvor muss jedoch noch angemerkt werden, dass im Rahmen der empirischen Analysen in Kapitel 5 aus sachlogischen Gründen auch lineare Regressionsmodelle ohne Konstante entwickelt werden. Dieser Hinweis ist relevant, da bei einer Regression ohne Konstante das Bestimmtheitsmaß R^2 nicht auf das Intervall $[0;1]$ normiert wird und daher seine Interpretation nicht möglich ist. Während bei einer linearen Regression mit Konstante die geschätzte Gerade durch den Schwerpunkt der Punktwolke gelegt wird (und die y-Achse entsprechend dieser Konstante schneidet), verläuft sie ohne Konstante zwangsweise durch den Nullpunkt. Je nach Aufgabenstellung kann dieser Verlauf der Geraden durch den Nullpunkt aus inhaltlichen Gesichtspunkten aber gewollt sein. Die Bestimmtheitsmaße werden deswegen in den entsprechenden Regressionen nur der Vollständigkeit halber angegeben, sie können jedoch nicht als Gütekriterium für die Schätzungen oder zum Vergleich mit anderen Regressionsergebnissen herangezogen werden.

Logistische Regression

Im Gegensatz zur linearen Regression dient die logistische Regression der Untersuchung diskreter Variablen, im empirischen Teil der Arbeit sind dies Variablen mit binären, also dichotomen Ausprägungen. Für die Eintrittswahrscheinlichkeit P der N Beobachtungen der binären Variablen Y gilt somit

$$P(y_n = 1) = 1 - P(y_n = 0) \ . \tag{3.9}$$

Daher gelten andere Voraussetzungen für die Durchführung der Regressionsanalyse, da hier beispielsweise keine Homoskedastizität (auch Varianzhomogenität genannt) vorliegt. Auch kann die Normalverteilung der Residuen

nicht unterstellt werden, die bei OLS-Schätzungen zur Anwendung der üblichen Teststatistiken erforderlich ist. Während bei stetigen Variablen die Verteilung im Intervall $[-\infty; +\infty]$ angenommen wird, treten bei binären Variablen mit nur zwei Ausprägungen weder eine Normalverteilung noch eine hinreichende Streuung auf.

Werden nun Werte einer solchen Variablen mittels linearer Regression geschätzt, so kann es durchaus passieren, dass sich die Schätzergebnisse außerhalb des Intervalls $[0; 1]$ befinden. Wird hingegen basierend auf einer nicht beobachteten latenten Variablen

$$z = \beta_0 + \sum_{i=1}^{I} \beta_i x_i \tag{3.10}$$

mit der logistischen Funktion[19]

$$P = \frac{e^z}{1 + e^z} = \frac{1}{1 + e^{-z}} \tag{3.11}$$

eine andere Verteilungsannahme getroffen, so ist sichergestellt, dass die Ergebnisse zwischen null und eins liegen, da

$$P(-\infty) = 0 \text{ und } P(+\infty) = 1 \tag{3.12}$$

gilt, darüber hinaus ist

$$P(0) = \frac{1}{2} \ . \tag{3.13}$$

Das Problem wird in der Logistischen Regression durch eine Transformation der abhängigen Variablen P $(y_n = 1)$ gelöst, indem die Eintrittswahrscheinlichkeit $P(y = 1)$ ins Verhältnis zu ihrer Gegenwahrscheinlichkeit $P(y = 0) = 1 - P(y = 1)$ gesetzt wird. Dieser Quotient entspricht den Chancen *(Odds)*[20] für $y = 1$ gegenüber $y = 0$ in der Form

$$Odds(y = 1) := \frac{P(y = 1)}{P(y = 0)} = \frac{P(y = 1)}{1 - P(y = 1)} \ , \tag{3.14}$$

[19] Hierbei sei $e \approx 2,718$ die Eulersche Zahl.

[20] Bei Sportwetten werden die Gewinnquoten in dieser Form berechnet, die Schreibweise variiert hingegen je nach Kulturraum. Für $P(y = 1) = 0,6$ gilt beispielsweise eine Chance von $\frac{0,6}{0,4} = 1,5$.

deren Wertebereich im Intervall $[0; +\infty]$ liegt. Um für die Schätzungen einen unbeschränkten Wertebereich erhalten zu können, werden diese Odds durch Logarithmierung in die sogenannten *Logits* transformiert mit

$$Logit(y = 1) := ln(Odds(y = 1)) \overset{(3.14)}{=} ln\frac{P(y = 1)}{1 - P(y = 1)} \ , \tag{3.15}$$

deren Wertebereich das Intervall $[-\infty; +\infty]$ abdeckt. Aus dieser Umformung folgt dann die Regressionsgleichung

$$Logit(y = 1|X_i = x_i) = \beta_0 + \sum_{i=1}^{I} \beta_i X_i \overset{(3.10)}{=} z \ , \tag{3.16}$$

mit welcher die Regressionsgewichte zur Berechnung der Logits geschätzt werden können.

Die Interpretation der in diesem Schritt errechneten Regressionskoeffizienten erweist sich jedoch als schwierig, da die Regressoren X_i die Wahrscheinlichkeit $P(y = 1)$ weder direkt noch linear beeinflussen. Aus diesem Grund kann zum einen kein Vergleich zwischen den Regressionskoeffizienten vorgenommen werden und zum anderen nicht vom Einfluss einer Ausprägung x_i auf die Veränderung von $x_i + 1$ geschlossen werden. Daher werden über die Exponenzierung dieser Koeffizienten die sogenannten Effektkoeffizienten errechnet, so dass sich für die Regressionsgleichung

$$Odds(y = 1|X_i = x_i) \overset{(3.15)}{=} e^{Logit(y=1|X_i=x_i)} \overset{(3.16)}{=} e^z \tag{3.17}$$

ergibt. Die Effektkoeffizienten liegen, wie bei der Definition der Odds erwähnt, im Intervall $[0; +\infty]$ und wirken multiplikativ, das heißt, bei einem Anstieg von x_i um eins entspricht ein Koeffizient von 1,5 einer Erhöhung um 50 %, ein Koeffizient von 0,8 einer Senkung um 20 %. Allgemein bedeuten Koeffizienten $e^{b_i} < 1$ einen negativen und $e^{b_i} > 1$ einen positiven Einfluss. Nach einer weiteren Transformation können die Einflüsse der logistischen Regression als Einflüsse auf Wahrscheinlichkeiten dargestellt werden mit

$$P(y = 1|X_i = x_i) \overset{(3.11)}{=} \frac{e^z}{1 + e^z} \tag{3.18}$$

und sind dann in der Interpretation vergleichbar mit den Ergebnissen einer linearen Regression.

Im Gegensatz zur Ermittlung der kleinsten Quadrate bei der OLS-Schätzung werden die Parameter bei der logistischen Regression auf Basis des *Maximum-Likelihood-Verfahrens* geschätzt. Bei diesem gilt es, die Wahrscheinlichkeit *(Likelihood)* so zu maximieren, dass die Koeffizienten der Regressoren die abhängige Variable richtig wiedergeben, also die Likelihood-Funktion

$$L = \prod_{n=1}^{N} \left(\frac{e^z}{1+e^z} \right)^{y_n} \cdot \left(1 - \frac{e^z}{1+e^z} \right)^{1-y_n} \tag{3.19}$$

zu maximieren.

Für die Bewertung der Qualität einer Logit-Schätzung stehen verschiedene Gütekriterien zur Auswahl, so gibt es analog zum Bestimmtheitsmaß der linearen Regression mit dem sogenannten Pseudo-R^2 eine Methode zur Bewertung der Qualität der Schätzung. Bei der Präsentation der Resultate von Logit-Schätzungen in Abschnitt 5.3 wird das oft verwendete Pseudo-Bestimmtheitsmaß von McFadden

$$R^2 = 1 - \frac{ln\ L_V}{ln\ L_0} \tag{3.20}$$

angegeben, dabei ist L_0 der Wert der Likelihoodfunktion des Nullmodells mit Konstante und L_V der Wert Likelihoodfunktion des vollständigen Modells. Unterscheiden sich die beiden Modelle nur unerheblich, ergibt sich für den Quotient ein Wert nahe eins, so dass das McFadden-R^2 bei ungefähr null liegt, während bei großen Unterschieden auch Werte nahe eins möglich sind. Als gute Werte für das Pseudo-Bestimmtheitsmaß können gemäß Backhaus et al. (2006) bereits Ergebnisse ab 0,2 bis 0,4 angesehen werden.

Neben dem Pseudo-R^2 nach McFadden wird bei den entsprechenden Regressionsergebnissen der logarithmierte Wert der Likelihood-Funktion des vollständigen Modells ($ln\ L_V$) angegeben.

Schrittweise Regression

Zur Entwicklung eines Regressionsmodells müssen zunächst aus den verfügbaren Variablen diejenigen Regressoren ausgewählt werden, für die eine inhaltlich kausale Einflussnahme auf die abhängige Variable sinnvoll erscheint. Aus der Berechnung ergibt sich dann im Anschluss, welche dieser Variablen

einen signifikanten Einfluss haben. Um nun aus den ausgewählten Variablen all diejenigen zu erhalten, die ein bestimmtes Signifikanzniveau erreichen, gibt es verschiedene automatisierte Berechnungsverfahren. Die schrittweise Regression vereinbart dabei als eine Kombination von Vorwärtsauswahl und Rückwärtsauswahl die Eigenschaften zweier weiterer Auswahlverfahren, indem sie deren Potential nutzt und die Nachteile der beiden Vorgehensweisen berücksichtigt.

Bei der *Vorwärtsauswahl* werden zunächst alle vorausgewählten K_v Variablen in einen bivariaten Zusammenhang zur unabhängigen Variablen gesetzt und anhand eines zuvor festgelegten Kriteriums wie eines Signifikanzniveaus diejenige Variable ausgewählt, welche dieses Kriterium am besten erfüllt. Diese Variable wird nun in das Regressionsmodell aufgenommen, danach wird in einer multivariaten Regression überprüft, welche der verbleibenden $(K_v - 1)$ Variablen zusätzlich unter den gleichen Bedingungen in das Modell aufgenommen werden kann. In jedem Iterationsschritt wird überprüft, welche weitere Variable in das Regressionsmodell einfließen kann, bis im k_v-ten Durchgang keine der verbleibenden $(K_v - k_v + 1)$ Variablen mehr aufgenommen wird.

Die *Rückwärtsauswahl* entspricht im Prinzip der Umkehrung dieser Vorgehensweise, so werden alle ausgewählten K_r Variablen in ein multivariates Regressionsmodell aufgenommen und wie in der Vorwärtsauswahl anhand eines Kriteriums überprüft. Wenn nicht alle Variablen das Kriterium erfüllen, wird die Variable mit dem schlechtesten Signifikanzwert aus dem Modell entfernt. Auch hier wird iterativ vorgegangen, bis im (k_r)-ten Schritt alle noch im Modell enthaltenen $(K_r - k_r + 1)$ Variablen das gewünschte Signifikanzniveau erreicht haben.

Als grundlegender Nachteil sowohl der Vorwärts- als auch der Rückwärtsauswahl muss die starre Vorgehensweise angesehen werden, die in der dynamischeren *Schrittweisen Regression* flexibler mit Veränderungen seitens der Signifikanzniveaus umgeht. So werden analog zur Rückwärtsauswahl bei der rückwärts durchgeführten schrittweisen Regression zunächst alle vorausgewählten Variablen in das erste Regressionsmodell aufgenommen und wenn nötig die Variable mit dem schlechtesten Signifikanzwert aus dem Modell entfernt. Bei jedem Iterationsschritt wird allerdings nicht nur überprüft, ob

einer der noch im Modell enthaltenen Regressoren insignifikant geworden ist, sondern auch, ob eine der bereits ausgeschlossenen Variablen im aktuellen Regressionsmodell wieder signifikant werden würde. Ist dies für eine oder mehrere Variablen der Fall, so würde(n) diese im nächsten Iterationsschritt wieder berücksichtigt werden.

Aus diesem Grund wird bei der schrittweisen Regression je ein Signifikanzniveau zur Einbeziehung und zum Ausschluss von Variablen angegeben, wobei ersteres den kleineren Wert besitzen muss. Analog können bei der vorwärts durchgeführten schrittweisen Regression Variablen aus dem Modell entfernt werden, wenn sie das vorgegebene Signifikanzniveau nicht mehr erfüllen. Somit kann bei beiden Verfahren der schrittweisen Regression das Zusammenspiel der Variablen auf der Suche nach einem guten Erklärungsmodell besser berücksichtigt werden.

Nach dem Überblick über die methodischen Grundlagen soll im folgenden Kapitel nun ein Einblick in die Datenbasis gegeben werden.

Kapitel 4

Datenbasis

Den empirischen Untersuchungen dieser Arbeit wird ein Datensatz zugrunde gelegt, welcher im Rahmen der vorliegenden Arbeit in den vergangenen Jahren erstellt wurde. Dabei wurde die Studie, aus welcher die Daten hervorgegangen sind, speziell an die Anforderungen der *Contingent Valuation* Methode angepasst.

Der im Rahmen einer Umfrage bei Unternehmen der IKT-intensiven Dienstleistungsbranche entwickelte Datensatz soll einen Einblick geben, wie die befragten Unternehmen die Bedrohungslage durch Schadprogramme einschätzen und wie hoch ihre Zahlungsbereitschaft zur Eindämmung dieser Gefahr ist. Des Weiteren sollen die Resultate Auskunft darüber geben, wie sehr die Unternehmen in den vergangenen Jahren mit der Bedrohung durch Malware selbst konfrontiert sowie von der immer größer werdenden Flut von Spam-Mails betroffen waren.

Gleichzeitig geben die Daten Einblick, welche Maßnahmen die befragten Unternehmen zu ihrem Schutz vor Gefahren aus dem Internet ergreifen und wie es um ihre IT-Sicherheit bestellt ist. Diese Zusammenhänge sind vor Allem vor dem Hintergrund interessant, dass die Branche durch ihre IKT-nahe Ausrichtung besonders von der Zuverlässigkeit ihrer IT-Struktur und somit der Gewährleistung der IT-Sicherheit abhängig ist. Die Entwicklung des Fragebogens und des daraus entstandenen Datensatzes wird auf den folgenden Seiten vorgestellt und näher erläutert.

4.1 ZEW Konjunkturumfrage

Das Zentrum für Europäische Wirtschaftsforschung (ZEW) in Mannheim führt mit der „ZEW Konjunkturumfrage“ regelmäßig eine Befragung von Unternehmen aus der IKT-Branche durch. Diese Befragung wird seit dem ersten Quartal 2002 vierteljährlich durchgeführt und ist der direkte Nachfolger einer vierteljährlichen Befragung von unternehmensnahen Dienstleistern aus dem Zeitraum 1994 (2. Quartal) bis Ende 2001. Seit 2002 liegt der Fokus gemäß der Projektseite des ZEW-Branchenreport auf den Dienstleistern der Informationsgesellschaft.

In Ermangelung einer allgemein akzeptierten Definition zur Abgrenzung des IKT-Sektors orientiert sich die Forschungsgruppe Informations- und Kommunikationstechnologien des ZEW an der Definition der OECD[1]. Die Bereiche Software und IT-Dienste, IKT-Handel sowie Telekommunikationsdienstleister zählen zu den IKT-Dienstleistern im engeren Sinn, zu den „wissensintensiven Dienstleistern“ gehören gemäß der Projektseite jene „Branchen, die Expertenwissen, Informationen, Problemlösungsansätze, Beratungs-, Forschungs- und Entwicklungsleistungen anbieten“ und „[sich] in ihrer Leistungserstellung [...] durch eine hohe Intensität an IKT und durch eine hohe Forschungs- und Entwicklungs-Intensität [auszeichnen]“. Dies sind im Einzelnen die Bereiche Steuerberatung und Wirtschaftsprüfung, Unternehmensberatung, Architekturbüros, technische Beratung und Planung, Forschung und Entwicklung sowie Werbung. Eine genauere Aufschlüsselung findet sich in Anhang A.

Bei der ZEW Konjunkturumfrage handelt es sich der Dokumentation von Margit Vanberg (2003) zufolge um eine geschichtete Zufallsstichprobe, deren Schichtungskriterien die neun Branchen,[2] der regionale Standort (West-/Ostdeutschland) und die Unternehmensgröße sind. Bei der Auswertung der Antworten erfolgt eine Gewichtung anhand der Unternehmensumsätze, um die relative wirtschaftliche Bedeutung eines jeden Unternehmens in die Be-

[1] Organisation für wirtschaftliche Zusammenarbeit und Entwicklung *(**O**rganisation for **E**conomic **C**o-operation and **D**evelopment).*

[2] In der Datenbasis der von Kaiser (1999) beschriebenen Befragung der unternehmensnahen Dienstleister waren es zehn Branchen.

wertung einfließen zu lassen. Darüber hinaus wird zur Herstellung der Repräsentativität die realisierte Stichprobe auf Basis der Schichtungszellen auf die Grundgesamtheit hochgerechnet.

Im Rahmen der in Zusammenarbeit mit dem Verband der Vereine Creditreform durchgeführten Erhebung des ZEW werden in jeder Welle ca. 4.000 Unternehmen aus den IKT-intensiven Dienstleistungsbranchen in Deutschland befragt, von denen sich ungefähr 1.000 Unternehmen regelmäßig an der Befragung beteiligen.

4.1.1 Aufbau des Fragebogens

Der Fragebogen der ZEW/Creditreform-Umfrage besteht aus zwei Teilen, der erste Teil der Umfrage, der sogenannte „Konjunkturteil“, behandelt dabei einen gleichbleibenden Fragenblock. In ihm geht es um Fragen zur Geschäftsentwicklung gegenüber dem vergangenen Quartal und die voraussichtliche Entwicklung im Folgequartal, wie um die Umsatzveränderung des Unternehmens. Darüber hinaus werden Fragen zur aktuellen und zukünftigen Entwicklung der Preise und Ertragslage, der Nachfrage nach Dienstleistungen des Unternehmens und zum Personalbestand gestellt.

Die Beantwortung der Fragen erfolgt zum Großteil auf einer 3-Punkte-Likert-Skala, beispielsweise lauten zur Frage „Ist der Umsatz Ihres Unternehmens...“ die möglichen Antworten „gestiegen“, „gleich geblieben“ und „gesunken“. Zusätzlich wird bei der Umsatzentwicklung eine prozentuale Angabe der Umsatzveränderung erbeten.

Die zweite, von Ulrich Kaiser (1999) als „Sonderfragenteil“ bezeichnete Hälfte des Fragebogens setzt sich flexibel aus wechselnden Fragen zusammen, die teilweise in einer Befragungswelle einen inhaltlichen Schwerpunkt behandeln oder verschiedene thematische Bereiche abdecken. Dabei tauchen gewisse Fragen in bestimmten Abständen in der Erhebung auf, manche Fragen wiederholen sich auch unregelmäßig. Beispielsweise wird regelmäßig erhoben, ob und in welchem Umfang ein Unternehmen ausbildet, wie sich die Altersstruktur der Beschäftigten aufbaut oder welchen Ausbildungsstand das Personal aufweist.

4.2 Zahlungsbereitschaft für IT-Sicherheit

In Zusammenarbeit mit der IKT-Abteilung des ZEW wurde im ersten Quartal 2006 dieser zweite Teil des Fragebogens auf den Themenschwerpunkt IT-Sicherheit ausgerichtet.[3] Dabei waren die Fragen rund um die Erfassung der Zahlungsbereitschaften auf die Bedürfnisse der *Contingent Valuation* zugeschnitten. Die Kernfragen für die Ermittlung der Zahlungsbereitschaft für zwei Aspekte der IT-Sicherheit wurden wie folgt formuliert:

„Angenommen, Sie hätten keine Möglichkeit, einen eigenen Spamfilter einzurichten. Wie viel wären Sie bereit pro Jahr an eine europäische Institution zur Bekämpfung von Spam zu zahlen, um den Anteil der unerwünschten E-Mails (Spam) zu senken?“

Je nach Befragungsgruppe wurden die Teilnehmer der Studie nach ihrer Zahlungsbereitschaft (in Euro) für eine Senkung um 30 % bzw. 70 % oder für eine Senkung um 50 % bzw. 90 % gefragt. Die Fragestellung zu Schadprogrammen mit Viren und Trojanern als explizit genanntem Beispiel wurde analog formuliert. Der Grund für die Frage nach unterschiedlichen Werten in verschiedenen Beobachtungsgruppen und nach jeweils zwei Werten pro Frage wird im Zusammenhang mit den vier verschiedenen Versionen von Fragebögen in diesem Abschnitt ab Seite 93 erläutert.

In seiner Arbeit zur Grundsatzdebatte der *Contingent Valuation* wurden von P. Portney (1994, S. 9) die sieben wichtigsten Richtlinien für die Entwicklung von CV-Studien zusammengefasst. Diese Übersicht wurde zur Bewertung der CV-Fragestellungen sowie der weiteren Umstände des Fragebogens zum Vergleich herangezogen, um eine methodisch bestmöglich an den Richtlinien orientierte Erhebung zu gewährleisten. Ziel der Evaluation des entwickelten Fragebogens war, in möglichst jedem Punkt den von Portney geschilderten Anforderungen zu entsprechen, sofern der Rahmen der Studie sowie die weiteren Umstände dies zuließen. Sofern dies unter den gegebenen Umständen nicht möglich war, werden die Gründe für die Abweichung von den Empfehlungen Portneys erläutert.

[3] An dieser Stelle möchte ich noch einmal Irene Bertschek, Margit Vanberg und Katrin Schleife für ihre Unterstützung bei der Planung und Durchführung des Projekts danken.

Zuerst wurde erwähnt, man solle Anwendungen der *Contingent Valuation* eher auf persönliche Interviews stützen als auf telefonische Befragungen und sich auf diese wiederum eher verlassen als auf per Post verschickte Fragebögen. Bei einer regelmäßig durchgeführten Studie, welche in einer der Befragungswellen die CVM anwendet, sollte sich dies in Bezug auf das Antwortverhalten der Teilnehmer jedoch weniger negativ auswirken als bei einer Zufallsstichprobe, in der beispielsweise zufällig ausgewählte Bürger angeschrieben werden.

Die zweite Anforderung, Zahlungsbereitschaften für die Verhinderung eines zukünftigen Ereignisses zu erfragen, anstatt sich nach einer geforderten Kompensation für ein vergangenes Ereignis zu erkundigen, wurde mit der Fragestellung erfüllt.

An dritter Stelle wurde empfohlen, CV-Studien im Referendumsformat durchzuführen, also Teilnehmer die Wahl treffen zu lassen, ob sie für oder gegen ein Programm stimmten, welches einen umweltbezogenen Nutzen im Austausch für höhere Steuern oder Produktpreise biete. Diese Empfehlung begründete die NOAA-Kommission damit, dass Individuen im Alltag häufig Entscheidungen dieser Art treffen müssten und ihre Antworten daher eher eine tatsächliche Bewertung reflektierten als beispielsweise bei *„open ended“*-Fragen, also offenen Fragen, welche eine maximale Zahlungsbereitschaft für jenes Programm erhöben.

Im Zusammenhang mit der vom ZEW durchgeführten Befragung konnte dieser Punkt jedoch nicht erfüllt werden, da es sich bei den Teilnehmern der Befragung um eine sehr heterogene Zielgruppe handelte. Da im Vorfeld nicht abzuschätzen war, von welchen Unternehmenseigenschaften die Zahlungsbereitschaften hauptsächlich abhängen könnten, war es auch nicht möglich, beispielsweise eine Zahlungsbereitschaft relativ zur Unternehmensgröße zu erfragen. Aus diesem Grund wurde die *Willingness to pay* in dieser Untersuchung in offenen Fragen erhoben, wie auch im Zusammenhang mit den Überlegungen zur Kontrolle des Embedding-Effekts ab Seite 98 noch näher erläutert wird.

Im Übrigen erfolgte Portneys Empfehlung, Zahlungsbereitschaften im Referendumsformat zu erfragen, aber auf Basis der Annahme, dass es sich bei den Teilnehmern einer Studie üblicherweise um normale Bürger ohne

besonderen kaufmännischen Hintergrund handelt, und nicht um Finanzentscheider mit entsprechender Erfahrung in ökonomischen Entscheidungen. Insofern ist die offene Frage nach einer selbst zu bestimmenden Zahlungsbereitschaft unter diesen Umständen vertretbar, da die Befragten entgegen der beschriebenen Begründung der NOAA-Kommission im Alltag durchaus regelmäßig Entscheidungen dieser Art treffen müssen. Ein weiterer Vorteil der hier notwendigen Vorgehensweise ist, dass die Schätzung durch den Wegfall der Extrapolation, wie bei Ludwig und Cook (2001, S. 214 ff) beschrieben, vereinfacht wird.

Der vierte Punkt wurde bei der Entwicklung der Fragestellung besonders beachtet, da in ihm ein Szenario gefordert wird, welches präzise und verständlich die zu erwartenden Effekte des betrachteten Programms beschreibt. Aus diesem Grund erfolgte eine detaillierte Beschreibung der Problemstellung, es wurde ein klares verständliches Szenario mit eindeutigen Definitionen vorgegeben, auch der zu erwartende Effekt war aus der Fragestellung eindeutig erkennbar und wurde außerdem auch zeitlich klar abgegrenzt. Darüber hinaus sollten für alle Unternehmen die gleichen Voraussetzungen geschaffen werden, indem angenommen wurde, es sei kein eigener Schutz vor den genannten Bedrohungen möglich. Bei der Problemlösungsstrategie wurde eine (namentlich nicht näher bezeichnete) fiktive europäische Institution gewählt, um der Internationalität der Gefahr gerecht zu werden, da es sich beim Internet und damit auch bei Spam und Malware um ein (fast) grenzenloses Phänomen handelt. Da im Vorfeld unklar war, ob und inwiefern sich die Frage nach der Zahlungsbereitschaft an erster Stelle negativ auf das Antwortverhalten auswirken könnte, wurde die Frage zwar relativ früh im Fragebogen, aber hinter einer Gruppe bereits häufiger gestellter Fragen positioniert, wie beispielweise dem Einsatz von E-Commerce.

Auch die fünfte Vorgabe basierte wie die Befürwortung des Referendumsformats auf der Annahme, dass es sich bei den Befragten nicht um Finanzentscheider handelt. Demnach müssten die Teilnehmer daran erinnert werden, dass ihre geäußerte Zahlungsbereitschaft den Geldbetrag reduziere, den sie für andere Dinge ausgeben könnten. Da Entscheidungen finanzieller Art in der vorliegenden Studie jedoch die tägliche Aufgabe der Befragten ist, wurde auf diese Erinnerung verzichtet.

Die sechste Anforderung war aufgrund des gewählten Szenarios nicht zutreffend, sondern bezog sich mit ihrer Fokussierung auf die Zahlungsbereitschaft für den Schutz von Natur auf den Haupteinsatzbereich der *Contingent Valuation.* Hier wird gefordert, den Probanden an Substitute für das zu bewertende Gut zu erinnern, als Beispiel wird gegeben, man solle den Probanden daran erinnern, dass es neben dem zu bewertenden Naturgebiet noch andere als Alternative gäbe. In dem entwickelten Szenario gibt es jedoch für die zu bewertende Reduzierung von Spam oder Malware nur die Alternative, keinen Schutz zu haben, und somit kein Substitut.

Im letzten Punkt der Empfehlungen der NOAA-Kommission wurde darauf hingewiesen, dass in weiteren Fragen die Gründe für die geäußerte Zahlungsbereitschaft herausgefunden werden sollten, um die bestimmenden Faktoren für die getroffene Entscheidung schätzen zu können. Der komplette zweite Teil des Fragebogens wurde auf diese Forderung ausgerichtet, so dass sie als erfüllt angesehen werden kann.

4.2.1 Embedding und Sequencing

Während bei den bisherigen Studien zu Kosten von Kriminalität die Quoten der Reduzierung von (Gewalt-)Verbrechen bei 10 % bzw. 30 % lagen, wurden für die vorliegende Studie zur Vermeidung von Malware und Spam bewusst höhere Werte gewählt. Bei der Verhinderung von Tötungsdelikten oder Raubüberfällen ist eine Senkung der Straftaten um 10 % durchaus eine Verbesserung, für die eine relativ hohe Zahlungsbereitschaft zu erwarten ist. Eine Reduzierung des Spam-Aufkommens um ein Zehntel ist aber ein „Tropfen auf den heißen Stein“, so dass hier neben extrem geringen Zahlungsbereitschaften viele „Protestantworten“ von 0 Euro zu erwarten wären. Dieser Effekt lässt sich vor Allem damit begründen, dass es bei Malware und Spam nicht wie bei Gewaltdelikten um die Reduzierung der Opferwahrscheinlichkeit geht, sondern lediglich um die Opferhäufigkeit.

Demnach würde bei 52.949 Raubdelikten, welche gemäß der Polizeilichen Kriminalstatistik (PKS) im Jahr 2007 in Deutschland verübt worden sind, eine Reduzierung von 10 % eine Vermeidung von jährlich über 5.000 Raubüberfällen bedeuten, eine Zahl, die subjektiv als sehr hoch wahrgenommen

wird. Unter der Annahme, dass jeder Einwohner Deutschlands unter Außerachtlassung jeglicher sozioökonomischer Hintergründe mit der gleichen Wahrscheinlichkeit Opfer einer solchen Straftat werden würde und diese zur Anzeige brächte, lag die Opferwahrscheinlichkeit für einen Raub im Jahr 2007 bei ca. 0,06 %. Diese Wahrnehmung kann jedoch dadurch verzerrt werden, dass ein Proband bei der Frage nach einer Zahlungsbereitschaft für die Vermeidung solcher Gewaltdelikte an die Folgen eines solchen Raubüberfalls für das Opfer denkt, welches mit einer gewissen Wahrscheinlichkeit der Proband selbst sein könnte.

Dagegen ist bei 20 erhaltenen Spam-Mails pro Tag eine Reduzierung um täglich zwei Spam-Mails nicht weiter nennenswert, da der Empfänger nun immer noch 18 unerwünschte Nachrichten zu bearbeiten hätte, sei es durch das simple Löschen der E-Mails oder indem die Nachrichten gelesen oder zumindest überflogen werden. Eine nennenswerte Verbesserung in der subjektiven Wahrnehmung des Spam-Opfers würde sich auf diese Weise also nicht einstellen, da sich weder der tatsächliche (tägliche) Zeitverlust noch der Umfang der subjektiv wahrgenommenen Störung merklich verringern würden. Eine Vermeidung von zehn oder mehr Spams pro Tag würde sich hingegen schon deutlicher bemerkbar machen und wäre damit eine wahrnehmbare Verbesserung der persönlichen Spam-Situation. Während 18 der ursprünglich 20 Werbenachrichten noch immer als ein störender Nachteil der elektronischen Kommunikation empfunden werden würden, könnten zwei verbleibende Spam-Mails pro Tag eher als notwendiges Übel hingenommen werden. Aus diesem Grund wurden sowohl für Schadprogramme als auch für unerwünschte E-Mails relativ hohe Werte für die Reduzierung gewählt, um den Befragten eine tatsächlich erkennbare Verbesserung der Bedrohungslage bzw. Belästigungssituation zu präsentieren.

Der häufig in der Kritik stehende Embedding-Effekt, der als quantitatives *Nesting* gemäß Carson und Mitchell (1995) oftmals im Sinne eines *Scope*-Effekts auftritt, wurde beim Design der Studie berücksichtigt und sollte zusätzlich gewissermaßen durch eine Art Umkehrung des Effektes genutzt werden. Während in den bisherigen Studien zur Schätzung der Kosten von Kriminalität ein linearer Zusammenhang zwischen der Verbesserung um $n\,\%$ und um $100\,\%$ unterstellt wurde, ist in Verbindung mit den hier betrach-

teten Phänomenen eher davon auszugehen, dass die Zahlungsbereitschaft für höhere Vermeidungspotentiale überproportional steigt. Demnach sollte die Zahlungsbereitschaft für eine Reduzierung des Spam-Aufkommens um 50 % die Zahlungsbereitschaft für 10 % weniger Spam[4] um erheblich mehr als das Vierfache überschreiten.[5]

In den Fragebögen wurden daher bei beiden Fragen zur Zahlungsbereitschaft zwei Werte abgefragt, um ein Auftreten der hier beschriebenen CVM-typischen Effekte beobachten zu können. So sollte durch die Angabe von Wertepaaren einerseits ein Embedding-Effekt nachweisbar gemacht werden, wenn der Quotient eines Antwortpaares erheblich unter jenem der entsprechenden Senkungspotentiale lag. Gleichzeitig konnte durch diese Quotienten gezeigt werden, ob Unternehmen einer Verbesserung des Vermeidungsanteils einen überproportional höheren Wert beimaßen.

Zunächst sollten in zwei Versionen des Fragebogens unterschiedliche Wertepaare abgefragt werden, um mehr Punkte für die Schätzung einer Zahlungsbereitschaftsfunktion zu erhalten. Unter der impliziten Annahme, dass eine Vermeidung von 0 % einer Zahlungsbereitschaft von 0 Euro zugewiesen werden kann, wurden im Rahmen der Befragung die Zahlungsbereitschaften für 30 % und 70 % Verbesserung auf der einen Seite sowie 50 % und 90 % auf der anderen Seite erfragt. Auf diese Weise sollten fünf Punkte einer Funktion der Zahlungsbereitschaft errechnet werden, um eine theoretische Zahlungsbereitschaft für eine (nicht realisierbare) 100 %ige Vermeidung schätzen zu können.

Wäre nun der Quotient aus den geäußerten Zahlungsbereitschaften für 90 % und 50 % kleiner als $\frac{90}{50} = 1,8$, so läge in diesem Fall Embedding vor, wie anhand des Beispiels auf Seite 59 nachvollzogen werden kann. Hätte also ein Unternehmen Zahlungsbereitschaften von 2.000 Euro für eine 50 %ige sowie 2.500 Euro für eine 90 %ige Reduzierung von Spam angegeben, wäre bei einem Quotienten von 1,2 offensichtlich jenes Problem des Einbettens

[4] Dieser Wert dient nur der Veranschaulichung und wurde aus den oben genannten Gründen nicht abgefragt.

[5] Da zu erwarten ist, dass die Zahlungsbereitschaft für eine Reduzierung um 50 % erheblich über dem fünffachen Wert für die Zahlungsbereitschaft von 10 % Vermeidung liegt, sollte die Differenz über dem vierfachen Wert liegen.

eines Gutes in ein inklusiveres Gut eingetreten, da eine Vermeidung von 90 % ungefähr den doppelten monetären Wert haben sollte wie eine Reduzierung um die Hälfte.

Bei einem Quotienten von (erheblich) mehr als $1,8$ würde sich in diesem Zusammenhang ergeben, dass eine Reduzierung des Spam-Aufkommens um 90 % aus Sicht des teilnehmenden Unternehmens einen deutlichen größeren Mehrwert hätte als die Senkung um die Hälfte. Zahlungsbereitschaften von beispielsweise 2.000 Euro für 50 % weniger Spam sowie 5.000 Euro für 90 % würden damit bei einem Quotienten von $2,5$ die Vermutung stützen, dass der Wert der Spam-Vermeidung im oberen Bereich des Reduzierungspotentials überproportional steigt.

Ein möglicherweise auftretender Embedding-Effekt ließe sich demnach in der vorliegenden Studie durch das Abfragen von jeweils zwei Zahlungsbereitschaften für eine thematische Fragestellung innerhalb der zu Protokoll gegebenen Wertepaare für jeden einzelnen Teilnehmer identifizieren.

Auch die zweite von den Kritikern bemängelte Fehlerquelle musste in diesem Fragebogen berücksichtigt werden, da mit der Reduzierung des Aufkommens von Malware und von Spam nach mehr als nur einer Zahlungsbereitschaft gefragt wurde. Einem unbeobachteten Sequencing-Effekt wurde beim Design des Fragebogens vorgebeugt, indem die beiden Fragen je nach Bogen in vertauschter Reihenfolge abgefragt wurden. Auf diese Weise wurden aus den beiden Versionen zur Zahlungsbereitschaft für unterschiedliche Senkungspotentiale durch die Permutation der Fragen vier Versionen.

Durch die Generierung einer Variablen für die Versionsnummer konnte eine Indikatorvariable für die Reihenfolge der Fragen eingeführt werden. Folglich wurde sichergestellt, dass ein potentiell auftretendes Sequencing im Rahmen der Schätzung der Zahlungsbereitschaftsfunktion entdeckt werden würde, die unterschiedlichen Versionen der Fragebögen sind in Tabelle 4.1 dargestellt.

Ein möglicherweise auftretender Sequencing-Effekt ließe sich nun bei der gemeinsamen Schätzung der Antworten aus Version 1 und 4 für die Reduzierung um 30 % bzw. 70 % nachweisen, analog aus Version 2 und 3 für die Senkung um 50 % bzw. 90 %. Ergäbe die Indikatorvariable für die Reihenfolge der Fragestellungen einen signifikanten Unterschied für eine geäußerte

	Wertepaare	
Sequencing	30 % und 70 %	50 % und 90 %
erst Malware, dann Spam	Version 1	Version 2
erst Spam, dann Malware	Version 4	Version 3

Tabelle 4.1: Unterschiede zwischen den vier Versionen des Fragebogens

Zahlungsbereitschaft, so hätte die Reihenfolge der Fragen tatsächlich einen Einfluss auf das Antwortverhalten der Probanden. Dabei wären, wie bereits im Beispiel ab Seite 62 ausgeführt, beide Arten von Sequencing in der vorliegenden Studie denkbar.

Die an zweiter Stelle geäußerte Zahlungsbereitschaft könnte demnach geringer ausfallen, als wenn sie an erster Stelle erfragt worden wäre, so dass dann die von Diamond und Hausman (1994) angesprochenen Einkommenseffekte zuträfen.

Nach der Äußerung einer Zahlungsbereitschaft für einen Aspekt der IT-Sicherheit müsste die teilnehmende Person demnach erneut über einen Geldbetrag nachdenken, nachdem sie bereits zuvor „Geld ausgegeben“ hätte. Da aber bereits Geld aus einem imaginären Budget des Probanden entnommen wurde, könnte die zweite Zahlungsbereitschaft nun geringer ausfallen, als wenn in der Vorstellung des Teilnehmers noch das volle Budget zur Verfügung stünde.

Auch wenn diese Erscheinungsform des Sequencing gemäß Carson et al. (1998) dem üblicherweise feststellbaren Phänomen entspräche, wäre im Zusammenhang mit der hier vorliegenden Thematik der umgekehrte Fall des Sequencing denkbar. So könnte die Frage nach der Zahlungsbereitschaft für die Eindämmung der Gefahren durch Malware im Speziellen die Probanden für die Bedrohungen aus dem Internet im Allgemeinen sensibilisieren. Dadurch wiederum könnten die Teilnehmer also für die Bekämpfung von Spam eine höhere Zahlungsbereitschaft äußern als sie es tun würden, wenn ihnen nicht durch die zuvor gestellte Frage zu Viren und Würmern das Gefahrenpotential des Internets vor Augen gehalten worden wäre.

Letzten Endes ist durch die Erhebung zweier Zahlungsbereitschaften die Möglichkeit des Sequencing gegeben, dies kann jedoch im Falle des Auftretens durch den Vergleich zwischen den Versionen der Fragebögen entdeckt werden.

4.2.2 Offene Fragen statt Referendum

Obwohl die NOAA-Kommission in ihren Empfehlungen zur Gestaltung von *Contingent Valuation*-Studien dazu rät, die Fragen nach Zahlungsbereitschaften nicht in offener Form zu stellen, sondern wenn möglich im Referendumsformat, fiel hier aus mehreren Gründen die Entscheidung für die Verwendung offener Fragen. So waren *a priori* weder die entscheidenden Einflussfaktoren für die Zahlungsbereitschaft noch die zu erwartenden Wertebereiche dieser Zahlungsbereitschaften pro messbarer Referenzeinheit wie beispielsweise dem Umsatz bekannt. Es konnte also lediglich vermutet werden, dass große Unternehmen absolut eine (wesentlich) höhere Zahlungsbereitschaft äußern als kleine Betriebe, relativ zur Mitarbeiterzahl aber ein Skaleneffekt bei den Investitionen in IT-Sicherheit und damit voraussichtlich auch bei der Zahlungsbereitschaft auftreten kann. Insofern hätte eine Referendums-Befragung mit absoluten Zahlungsbereitschaften keinen Sinn ergeben, eine Erhebung mit relativem Bezug hätte jedoch bereits im Vorfeld Kenntnisse über die besten erklärenden Variablen für die Zahlungsbereitschaft verlangt. So dürfte zwar die Befragung einer relativ homogenen Gruppe von Teilnehmern wie beispielsweise von Steuerzahlern im Referendumsformat empfehlenswert sein, bei einer so heterogenen Beobachtungsgruppe wie Unternehmen verschiedenster Größen sollten hingegen offene Fragen bessere Ergebnisse erzielen.[6]

Neben den im Mittelpunkt stehenden Fragen zur Zahlungsbereitschaft für die Bekämpfung von Schadprogrammen und Spam wurden 14 weitere Fragen gestellt, deren Antworten zur Schätzung der Zahlungsbereitschaftsfunktion herangezogen werden sollten. Dabei wurden in dieser Welle viele Fragen zum ersten Mal speziell im Zusammenhang mit der *Contingent Valuation* gestellt, bestimmte Fragen, die sich zuvor schon regelmäßig wiederholt hatten, wurden aber auch für diesen Fragebogen erneut aufgegriffen. Zwei der Fragen behandelten die Unternehmensgröße, so wurde nach dem Umsatz des Unternehmens (in Tausend Euro) und der Anzahl der Mitarbeiter gefragt. Die verbleibenden 12 Fragen deckten verschiedene Themengebiete zur Rolle der Informations- und Kommunikationstechnologien sowie der IT-Sicherheit ab.

[6] In der vorliegenden Studie liegen die 10 %- bzw. 90 %-Perzentile für die Mitarbeiter bei 4 bzw. 140, für die angegeben Umsatzzahlen bei 149 Tausend bzw. 20 Millionen Euro.

Inwiefern das Unternehmen von der Informationstechnologie abhängig ist, wurde durch Fragen nach dem Anteil der Mitarbeiter mit Computerarbeitsplatz und der Rolle des elektronischen Handels, des sogenannten *„E-Commerce“* eruiert. Diese beiden Themengebiete waren bereits regelmäßig Bestandteil der Konjunkturumfrage und wurden bislang im zweiten Quartal eines jeden Jahres behandelt. Bei der Frage nach den Computerarbeitsplätzen ging es dabei um den Anteil der Beschäftigten, welche den überwiegenden Teil ihrer Arbeit an einem PC, Laptop, Terminal oder einer Workstation erledigen.

Mit dem Einsatz von E-Commerce beschäftigten sich gleich drei Fragestellungen, so sollte das teilnehmende Unternehmen zunächst darüber Auskunft geben, ob es in seinen Geschäftsbeziehungen die Möglichkeit nutze, Bestellungen über das Internet von anderen Unternehmen bzw. von Endkunden anzunehmen oder nicht. Im zweiten Schritt wurde nach dem Umsatzanteil mit E-Commerce am Gesamtumsatz aus dem Jahr 2005 gefragt, hier konnte mit „nicht zutreffend“ auch gekennzeichnet werden, dass man selbst keine Möglichkeiten des elektronischen Handels anbietet. In der dritten Frage ging es um die Nutzung der Möglichkeit, selbst Bestellungen über das Internet aufzugeben.

Die zweite Gruppe von Fragen behandelte die Qualifikation der Mitarbeiter sowie die IT-(Sicherheits-)Kompetenz des Unternehmens. Nach der Erhebung der Anzahl der Mitarbeiter mit einer Ausbildung oder einem Studium im IT-Bereich wurden die Zahlen der Mitarbeiter ermittelt, die hauptsächlich (nur) für Systemadministration, (nur) für IT-Sicherheit sowie sowohl für Administration als auch für IT-Sicherheit beschäftigt sind. Dabei spielt die Frage nach der speziellen Aufgabenverteilung ebenso eine Rolle im Problembewusstsein des Unternehmens in Fragen der IT-Sicherheit wie die Frage nach externer Unterstützung in der IT-Sicherheit. So wurde thematisiert, ob sich das Unternehmen bei Fragen der IT-Sicherheit von externer Seite beraten lasse, und ob es die Administration des IT-Bereichs teilweise oder komplett an externe Unternehmen ausgelagert habe, also ein *„Outsourcing“* des IT-Bereichs betreibe. Die Frage zur IT-Beratung wurde in ähnlicher Weise bereits in einer Befragungswelle zwei Jahre zuvor im Rahmen der Inanspruchnahme externer Beratungsdienstleistungen gestellt.

Die folgende Frage zielte noch mehr auf das Problembewusstsein des Unternehmens ab, indem sie sich auf die Weiterbildung von Administratoren und Anwendern im Bereich IT-Sicherheit sowie auf die Aufklärung der Anwender über mögliche Gefahren aus dem Internet bezog. Hier konnten die Unternehmen erklären, ob sie ihren Mitarbeitern eine diesbezügliche Fortbildung ermöglichen oder ob sie solche Maßnahmen nicht unterstützen.

Der vorletzte Fragenblock konzentrierte sich darauf, inwiefern das Unternehmen mit der Problematik von Spam und Malware konfrontiert war. Zuerst sollte geschätzt werden, wie hoch der derzeitige Anteil an Spam am eigenen täglichen Mail-Aufkommen sei, bevor die Gretchenfrage nach Vorfällen durch Schadprogramme gestellt wurde.

> *„Gab es in Ihrem Unternehmen bereits Vorfälle durch Schadprogramme (z.B. Viren, Trojaner)?“*

Neben dem Hinweis, dass Mehrfachnennungen möglich seien, wurden als Antwortmöglichkeiten die Jahre 2005 und 2004 sowie der Zeitraum „vor 2004“ gegeben, zur Vermeidung unnötiger Missings wurde auch „Nein, noch nie“ zur Wahl gestellt. Dabei war die Frage bewusst allgemeiner gehalten als die inhaltlich ähnliche Frage aus dem ersten FAZIT-Fragebogen[7] aus dem Frühjahr 2005 *„Hatten Sie in letzter Zeit auf Grund eines Befalls durch Viren, Trojaner, Würmer, etc. Datenverluste zu verzeichnen?“,* da diese Spezifikation einerseits nur eine (Schadens-)Facette von Malware berücksichtigte und andererseits eben diese Schadensform schon zum damaligen Zeitpunkt eher in den Hintergrund getreten war. Insofern war bei der Fragestellung wichtig, ob ein Unternehmen einen nicht genauer definierten Vorfall mit Schadprogrammen hatte, wohl aber bereits wissentlich Opfer dieser Bedrohung aus dem Internet war und sich somit der Gefahr bewusst.

Auf eine Auswahlmöglichkeit im Sinne von „keine Angabe“ wurde wegen des knappen für diese Fragestellung zur Verfügung stehenden Platzes

[7]Das gemeinnützige „**F**orschungsprojekt für **A**ktuelle und **Z**ukunftsorientierte **I**nformations- und Medien**T**echnologien und deren Nutzung in Baden-Württemberg“ wird von der MFG Stiftung Baden-Württemberg in Stuttgart getragen und in Zusammenarbeit mit dem Zentrum für Europäische Wirtschaftsforschung (ZEW) in Mannheim und dem Fraunhofer-Institut für System- und Innovationsführung in Karlsruhe durchgeführt.

auf dem Fragebogen verzichtet. Auch sollte den Teilnehmern nicht durch das Anführen dieser Antwortmöglichkeit das Gefühl vermittelt werden, dass es akzeptabel oder gar gewünscht sei, wenn zu dieser Frage keine Angaben gemacht werden würden. Daher wurden jene Unternehmen, welche keine Angaben zu Vorfällen machen wollten oder konnten, bei dieser Frage in den Missings abgebildet.

Bei der Erstellung des Fragebogens war noch nicht abzusehen, von wie vielen Teilnehmern diese unangenehme Frage beantwortet werden würde. Aus diesem Grund wurde das heikle Thema erst kurz vor Ende des Fragebogens angesprochen, um die teilnehmenden Unternehmen nicht zu früh abzuschrecken, so dass im Falle eines Abbruchs der Beantwortung des Fragebogens immer noch möglichst viele Informationen eingetragen worden waren. Die Auswertung in Abschnitt 5.1 zeigt jedoch eine überraschend gute Antwortmoral bei dieser problematischen Thematik.

Zuletzt wurde nach dem Anteil für IT-Sicherheit am IT-Budget des Unternehmens aus dem Jahr 2005 gefragt, hier dienten die Resultate der ersten Welle der FAZIT-Unternehmensbefragung als Orientierungshilfe für die genaue Formulierung der Fragestellung und der zur Verfügung gestellten Antworten. Dabei wurden die Antwortklassen 1-5 % und 6-10 % übernommen, die Klassen 11-15 %, 16-20 %, 21-25 % und > 25 % wurden zu einer Klasse > 10 % zusammengefasst, da sich in der Auswertung von Irene Bertschek und Jörg Ohnemus (2005, S. 50) lediglich 10,1 % der Antworten auf jene vier Klassen verteilt hatten. Während die Antwortoption „weiß nicht“ ebenfalls gegeben war, wurde aufgrund der IT-Ausrichtung des betrachteten Wirtschaftssektors auf eine Antwort von 0 % Budget-Anteil verzichtet.

Im folgenden Kapitel erfolgt die Analyse des ZEW-Datensatzes mit dem Fokus auf den von den teilnehmenden Unternehmen geäußerten Zahlungsbereitschaften für die Reduzierung der Bedrohung durch Malware sowie der Belästigung durch Spam. In diesem Zusammenhang soll darüber hinaus festgestellt werden, welche Variablen auf die Zahlungsbereitschaft einen signifikanten Einfluss haben.

So wird die Frage geklärt, ob die Unternehmen, die bereits (wiederholt) Vorfälle mit Schadprogrammen hatten, eine höhere Zahlungsbereitschaft

äußern und möglicherweise auch einen größeren Anteil ihres IT-Budgets in IT-Sicherheit investieren. Ebenso kann die Abhängigkeit von der Zuverlässigkeit der IT diese Zahlungsbereitschaft positiv beeinflussen, beispielsweise bei einem höheren Anteil an PC-Arbeitsplätzen oder einem großen Umsatzanteil durch E-Commerce. Dagegen dürfte das Auslagern der IT-Administration keinen Einfluss haben, da es eigentlich keinen Unterschied machen dürfte, ob ein Unternehmen diese Leistung selbst erbringt oder gegen Bezahlung erbringen lässt.

Darüber hinaus sollen die Ergebnisse der Regressionen aufzeigen, welchen Einfluss beispielsweise der Anteil für IT-Sicherheit am IT-Budget auf die Wahrscheinlichkeit hat, von Schadprogrammen betroffen zu sein, und welche Faktoren mit dem Anteil der Spam-Mails am Mail-Aufkommen in Verbindung stehen.

Kapitel 5

Empirische Analyse

„If you spend more on coffee than on IT security, then you will be hacked. What's more, you deserve to be hacked."
White House Cybersecurity Advisor, Richard Clarke
Keynote speech at RSA Conference 2002

Deutliche Worte fand der damalige Top-Berater des US-Präsidenten für *IT-Security* am 19. Februar 2002, als er im Rahmen seiner *Keynote*-Rede auf der *RSA Data Security Conference* in San Jose (CA) Statistiken zitierte, nach denen Unternehmen durchschnittlich weniger als 0,0025 % ihres Umsatzes für IT-Sicherheit aufwendeten. Nach Angaben von ZDNet (2002) betonte Richard Clarke auf der weltweit größten Konferenz für Computersicherheit die Notwendigkeit einer Zusammenarbeit der Industrie zur Sicherung des Internets als Ganzem, und dass sich Unternehmen nicht nur um ihr eigenes kleines Stück Netz sorgen sollten. Dabei lobte er besonders die Anstrengungen, die einige Firmen der IT-Branche unternähmen, um besser auf die Belange der IT-Sicherheit zu achten.

Clarke äußerte weiterhin, die Terroranschläge vom 11. September 2001 hätten gezeigt, dass die Feinde der USA technisch versiert und hartnäckig seien, und stellte klar, die zukünftigen Feinde verstünden die [amerikanische] Technologie mindestens genauso gut wie sie [die USA] selbst. Außerdem verkündete er, Präsident George W. Bush habe im (damals) vorgeschlagenen

Staatshaushalt die Ausgaben für Informationssicherheit um 64 % auf 4 Mrd. US-Dollar erhöht und fügte hinzu, diese Erhöhung entspreche 8,1 % des Gesamtbudgets für Informationstechnologie.

Gemäß der vom ZEW in Baden-Württemberg durchgeführten FAZIT-Umfrage (2005) gaben 40,5 % der teilnehmenden Unternehmen im Jahr 2004 zwischen einem und fünf Prozent ihres IT-Budgets für IT-Sicherheit aus, 13,2 % der Befragten investierten zwischen sechs und zehn Prozent ihres IT-Haushalts, lediglich jeder zehnte Teilnehmer der Studie (10,1 %) lag darüber. Dagegen konnte (oder wollte) mit 23,3 % fast ein Viertel der Teilnehmer keine Auskunft über den Budget-Anteil der IT-Sicherheit ihres Unternehmens geben, 12,8 % gaben mit null Prozent sogar explizit an, überhaupt keine Mittel für IT-Sicherheit bereitzustellen.

Während die FAZIT-Umfrage sowohl das verarbeitende Gewerbe als auch die Dienstleister des IT- und Mediensektors (in Baden-Württemberg) untersuchte, fokussiert die vierteljährlich durchgeführte „ZEW Konjunkturumfrage“ auf die IKT-intensive Dienstleistungsbranche in Deutschland. Im ersten Quartal 2006 wurden im Rahmen der „ZEW Konjunkturumfrage“ ungefähr 4.000 Unternehmen zu verschiedenen Themen der IT-Sicherheit befragt, unter Anderem zum Anteil der Investitionen für IT-Sicherheit am gesamten IT-Budget.

Der Schwerpunkt des sogenannten Sonderfragenteils lag dabei in dieser Erhebungswelle erstmals komplett in diesem sensiblen Themenbereich, um eine ausreichend große Basis an Variablen für die geplante Schätzung der Zahlungsbereitschaft für IT-Sicherheit auf Basis der *Contingent Valuation* Methode sicherzustellen. Analog der üblichen Vorgehensweise bei der Anwendung dieser Methode sollten die Schätzergebnisse als Grundlage für die Berechnung der Kosten von nicht-marktfähigen Gütern dienen, in diesem Fall also jener Kosten, welche durch Schadprogramme sowie durch unerwünschte E-Mails verursacht werden.

Eine deskriptive Betrachtung der Datenbasis führt im ersten Abschnitt des Kapitels auf die Ergebnisse der Studie hin, bevor eine Faktorenanalyse in Abschnitt 5.2 erste Hinweise auf mögliche Zusammenhänge zwischen einzelnen, nicht direkt verknüpften Variablen gibt.

Die Resultate der Regressionen zur Zahlungsbereitschaft für die anteilige Reduzierung des Aufkommens von Malware und Spam werden in Abschnitt 5.3 vorgestellt, gefolgt von Überlegungen zur Zahlungsbereitschaft für die theoretische Senkung von einhundert Prozent und somit gewissermaßen der völligen Behebung des Problems. Im Anschluss werden die Regressionsergebnisse zu weiteren Fragestellungen präsentiert, welche im Zusammenhang mit der Studie erörtert wurden. Dabei werden mit dem Auftreten von Malware und dem Spam-Anteil am E-Mail-Aufkommen zunächst die Themenschwerpunkte behandelt, bevor die Ergebnisse zu ausgewählten Themen wie beispielsweise die Entscheidung für oder gegen IT-Outsourcing vorgestellt werden.

5.1 Deskription der Daten

An der Umfrage im Frühjahr 2006 nahmen 844 Unternehmen aktiv teil, damit liegt die Zahl der zur Verfügung stehenden Beobachtungen nahe der Anzahl an Unternehmen, welche sich üblicherweise an der Umfrage beteiligen. Für die Präsentation im „ZEW Branchenreport – Dienstleister der Informationsgesellschaft“ werden die Ergebnisse gemäß M. Vanberg (2003, S. 3) entsprechend der ökonomischen Bedeutung eines Unternehmens gewichtet und auf die Zellen der geschichteten Stichprobe hochgerechnet, um die Repräsentativität der realisierten Stichprobe zu gewährleisten.

Eine Gewichtung dieser Art wird im Rahmen der vorliegenden Arbeit nicht vorgenommen, da diese besonders bei den drei im Datensatz schwach besetzten Wirtschaftszweigen zu starken Verzerrungen führen könnte. Darin begründen sich in dieser Hochrechnung die Unterschiede, welche bei den Ergebnissen in diesem Abschnitt gegenüber den im „ZEW Branchenreport“ veröffentlichten Resultaten auftreten.

Die Wirtschaftszweige IKT-Handel, Telekommunikationsdienstleister sowie Forschung und Entwicklung sind in dieser Erhebung stark unterrepräsentiert. Aus diesem Grund werden die drei Wirtschaftszweige bei den Regressionen in Abschnitt 5.3 nicht weiter berücksichtigt, da für die geringe Zahl von Beobachtungen keine zuverlässigen Aussagen getroffen werden können. Bei mehr als der Hälfte der Unternehmen lag keine Zuordnung zu einem

Wirtschaftszweig	**Anz. Beob.**	**Hochrechnung**
Software und IT-Dienste	70	118
IKT-Handel	2	111
Telekommunikationsdienstleister	1	50
Steuerberatung und Wirtschaftsprüfung	90	108
Unternehmensberatung	63	91
Architekturbüros	90	111
Technische Beratung und Planung	28	75
Forschung und Entwicklung	3	92
Werbung	48	88
Missings	449	–

Tabelle 5.1: Beobachtungen sortiert nach Wirtschaftszweigen

Wirtschaftszweig vor, eine verlässliche Zuteilung anhand der Klassifikationsnummer von 1993 war aufgrund der in der Zwischenzeit erfolgten Umstrukturierung der Wirtschaftszweige nur bedingt möglich und wurde daher unterlassen. Die Hochrechnung in Tabelle 5.1 gibt an, mit welchem ungefähren Gewicht die beobachteten Unternehmen in eine repräsentative Umfrage hätten einfließen müssen.

Um einen ersten Überblick über mögliche Beziehungen zwischen Variablen zu gewinnen, wurde eine Korrelationsmatrix erstellt, welche auszugsweise in Tabelle 5.2 wiedergegeben wird. Dabei wurde bewusst auf die Darstellung von Zusammenhängen innerhalb von Variablengruppen verzichtet, die wie beispielsweise im Falle des E-Commerce im Fragebogen in einem Block zusammengefasst worden waren und bei welchen Interdependenzen offensichtlich sind. In der Tabelle sind lediglich Korrelationen von Variablen berücksichtigt, wenn sie auch Verknüpfungen zu Variablen anderer Fragen aufweisen. Weitere Korrelationen innerhalb von Frageblöcken werden bei Bedarf in den entsprechenden Unterabschnitten aufgezeigt. Bei einigen paarweisen Korrelationen liegen 748 Beobachtungen vor, da in diesen Fällen eine Variable aus einem Fragenblock zur Anzahl der Administratoren entstammt oder es sich um eine daraus generierte Variable handelt, dieser Fragenblock wurde einheitlich beantwortet, also ohne einzelne Missings.

	Ums2005	AnzMA	AnzIT	AnzAd	AnzITS	AntITS	AntSumAI
AnzMA	0,6492*						
	(638)						
AnzIT	0,4890*	0,6657*					
	(633)	(751)					
AnzAd	0,4020*	0,4978*	0,8985*				
	(630)	(748)	(749)				
AnzITS		0,5187*		0,4321*			
		(748)		(780)			
SumAdITS		0,5552*	0,8517*	0,9768*	0,5796*		
		(748)	(749)	(780)	(780)		
AntAd						0,6498*	0,7429*
						(748)	(748)
AntITS							0,6897*
							(748)
AntAdIT							0,6012*
							(748)

Erklärung: *Signifikanz zum 0,1 %-Niveau; Anz. Beob. in Klammern; Korrelationen $< \pm 0,3$ wurden nicht berücksichtigt

Tabelle 5.2: Korrelationsmatrix ausgewählter Variablen

Wie aus Tabelle 5.2 entnommen werden kann, ist der im Jahr 2005 erzielte Umsatz *(Ums2005)* nicht nur mit der Anzahl der Mitarbeiter *(AnzMA)* hoch korreliert, sondern auch mit der Anzahl der Mitarbeiter mit IT-Ausbildung oder -Studium *(AnzIT)* sowie der Anzahl der Administratoren *(AnzAd).* Der Grund für diesen Zusammenhang mit dem Umsatz ist in seiner relativ hohen Korrelation mit der Anzahl der Mitarbeiter zu sehen, die selbst wiederum mit beiden Variablen korreliert ist. Da beide Korrelationswerte für die Anzahl der Mitarbeiter zwischen 0,10 und 0,18 höher liegen als für den Umsatz, ist davon auszugehen, dass dieser Zusammenhang mit den IT-Spezialisten und Administratoren nur über die Mitarbeiterzahl zustande gekommen ist. Weiterhin ist die Größe des Personalbestands korreliert mit der Anzahl der Mitarbeiter, deren ausschließliche Aufgabe die IT-Sicherheit ist *(AnzITS),* und mit der Summe, die aus den drei Gruppen von Administrationskräften *(SumAdITS)* gebildet wurde. Für diese Werte ist, sofern vorhanden, nur ein geringer Zusammenhang mit den Umsatzzahlen zu vermuten, da der Korrelationswert von Umsatz und der Anzahl der Mitarbeiter für IT-Sicherheit nahe null liegt, zwischen dem Umsatz und der Summe aller Administratoren bei 0,27.

	Anteil am Personal				
Quantil	**AntIT**	**AntAd**	**AntITS**	**AntAdIT**	**AntSumAI**
Minimum ··· 25%	0	0	0	0	0
40%	0	⋮	⋮	⋮	1,00
50%	1,00				2,86
60%	5,00	0	0	0	4,55
75%	20,00	2,86	0,28	2,42	9,93
90%	61,54	11,11	5,00	9,09	23,08
95%	85,71	17,14	10,00	16,67	33,33
99%	100,0	33,33	33,33	40,00	83,33
Maximum	100,0	71,43	66,67	100,0	100,0
Anz. Beob.	751	748	748	748	748
Mittelwert	16,67	3,37	1,74	3,19	8,31
Std. Abw.	27,79	7,85	5,60	9,38	15,33

Tabelle 5.3: Anteil der IT-Fachkräfte und Administratoren (in Prozent)

Eine sehr hohe Korrelation besteht für die Anzahl der IT-Fachkräfte sowohl mit der Anzahl der Mitarbeiter (nur) für Administrationsaufgaben, als auch für die Summe aus den drei Administratorengruppen. Die Korrelation von fast 0,98 zwischen der Anzahl der Mitarbeiter, welche ausschließlich für reine Administrationstätigkeiten zuständig sind, und jener, welche neben der eigentlichen Administration auch oder nur Verantwortung für die IT-Sicherheit tragen, erklärt diesen Zusammenhang. So setzt sich die Summe der drei Gruppen von Administrationskräften hauptsächlich aus den Mitarbeitern zusammen, die sich nur mit der Administration beschäftigen und somit nicht für die Gewährleistung der IT-Sicherheit verantwortlich sind. Mit insgesamt 1.257 Personen stellen die Administratoren mit dem enger gefassten Aufgabenbereich der Administration den größten Anteil der Admin-Gruppe (58 %), die IT-Sicherheit ist für 398 Beschäftigte die einzige Aufgabe, für die Kombination beider Tätigkeiten sind 512 Personen zuständig.

Da die Anzahl der Mitarbeiter, die für verschiedene Administrationsaufgaben verantwortlich sind, eindeutig von der Größe des Personalbestands eines Unternehmens abhängig ist,[1] wurde in den weiteren Untersuchungen mit den Anteilen dieser Personengruppen am Personalbestand gerechnet.

[1]Diese Annahme wurde in drei Fällen durch bivariate Regressionen mit t-Werten > 15 bestätigt, im vierten Fall (nur für IT-Sicherheit beschäftigt) betrug der t-Wert 2,13.

Diese Abhängigkeit war bereits beim Design des Fragebogens vermutet worden, um jedoch Verzerrungen durch ungenaue Angaben zu vermeiden, wurde anstatt nach zumeist gerundeten relativen Anteilen in Abhängigkeit von der Mitarbeiterzahl nach absoluten Beschäftigtenzahlen gefragt. Für die drei Gruppen liegen die Mittelwerte zwischen 1,7 % und 3,4 %, so dass diese Annahme berechtigt war, bei der Frage nach Anteilen wären die Unternehmen vermutlich erheblich ungenauer mit ihren Angaben gewesen.[2] Diese Anteilswerte weisen ebenfalls teilweise Korrelationen untereinander auf, wie aus Tabelle 5.2 hervorgeht.

Fast die Hälfte der Unternehmen (48 %) verfügen über keine eigenen IT-Fachkräfte *(AntIT),* gemäß Tabelle 5.3 hat dennoch durchschnittlich jeder sechste Beschäftigte der IKT-Branche eine IT-Ausbildung oder ein IT-Studium absolviert. In jedem dritten Unternehmen beträgt dieser Anteil bis zu einem Viertel, dagegen setzt sich nur etwa ein Siebtel der Unternehmen mehrheitlich aus Mitarbeitern mit IT-Hintergrund zusammen. Im Mittel kann jeder sechste Beschäftige der IKT-nahen Branchen als IT-Fachkraft angesehen werden, während der Median beim Anteil des Personals mit IT-Ausbildung oder -Studium gerade einmal bei einem Prozent liegt. Abgesehen von den drei Wirtschaftszweigen, bei denen aufgrund der geringen Anzahl an Beobachtungen davon auszugehen ist, dass die teilnehmenden Unternehmen nicht repräsentativ für die Branche sind, unterscheiden sich die Mittelwerte nur wenig und liegen zwischen 13 % und 21 %.

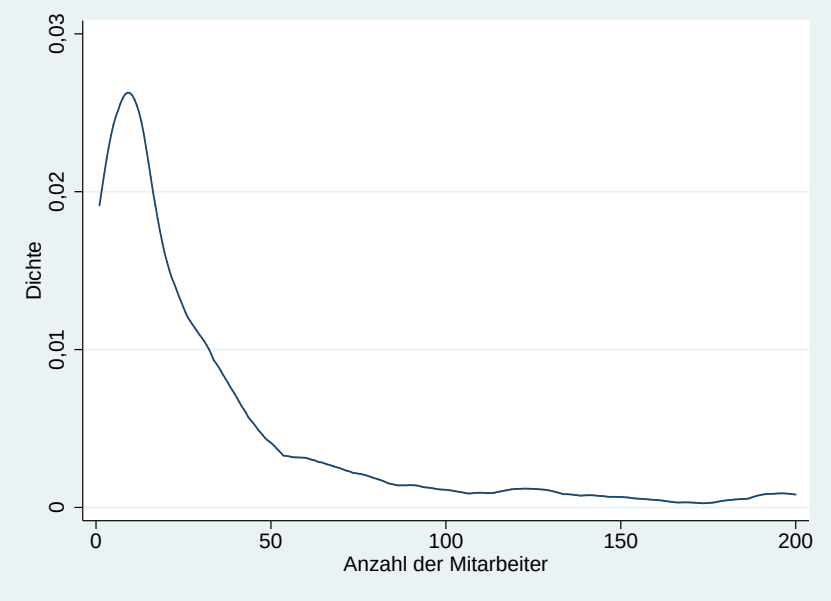
Beim Vergleich der Quantilswerte um den Median aus Tabelle 5.3 wird offensichtlich, dass einige Unternehmen Mitarbeiter für die Bereiche Administration und IT-Sicherheit beschäftigen *(AntSumAI bzw. Anteile der Teilgruppen),* die weder eine Ausbildung noch ein Studium im IT-Bereich abgeschlossen haben. Dies wird auch durch einen Blick auf die Abbildungen B.5 und B.6 in Anhang B verdeutlicht. So arbeiten mit 38 % nur in gut einem Drittel der befragten Unternehmen keine Personen als hauptamtliche Administratoren, obwohl von 48 % der Teilnehmer angegeben wurde, über keine qualifizierten IT-Fachkräfte zu verfügen. Eine Gegenüberstellung der beiden Mitarbeiterquoten ergibt, dass in 19 % der Fälle Personen für Administration

[2] Beispielsweise hätte ein Unternehmen mit 135 Mitarbeitern bei 2 Administratoren (1,48 %) als Anteil 1 % oder 2 % angeben können. Es wäre hierbei nicht zu erwarten gewesen, dass dieser Wert möglichst präzise als 1,5 % angegeben worden wäre.

und IT-Sicherheit verantwortlich sind, denen weder eine Ausbildung noch ein Studium im IT-Bereich zuteil wurde.

5.1.1 Unternehmensgröße

Ungefähr die Hälfte der befragten Unternehmen beschäftigt gemäß Abbildung 5.1 weniger als 20 Mitarbeiter, dementsprechend liegt der Median bei 20 Mitarbeitern. Bei einem Viertel liegt die Beschäftigtenzahl zwischen 20 und 49, das verbleibende Viertel hat mindestens 50 Personen beschäftigt. Immerhin 14 der 782 Unternehmen, die über ihre Mitarbeiterzahl Auskunft erteilt haben, gaben an, einen Personalbestand von 1.000 Mitarbeitern oder mehr zu haben, zwei davon liegen sogar im Bereich zwischen 10.000 und 14.000 Beschäftigten. Im Mittel sind bei einem Unternehmen 135 Mitarbeiter beschäftigt, dieser hohe Mittelwert gegenüber dem Median ist durch die Ausreißer der Großunternehmen bedingt, lediglich bei 80 Unternehmen liegt die Zahl der beschäftigten Arbeitnehmer über dem Mittelwert.

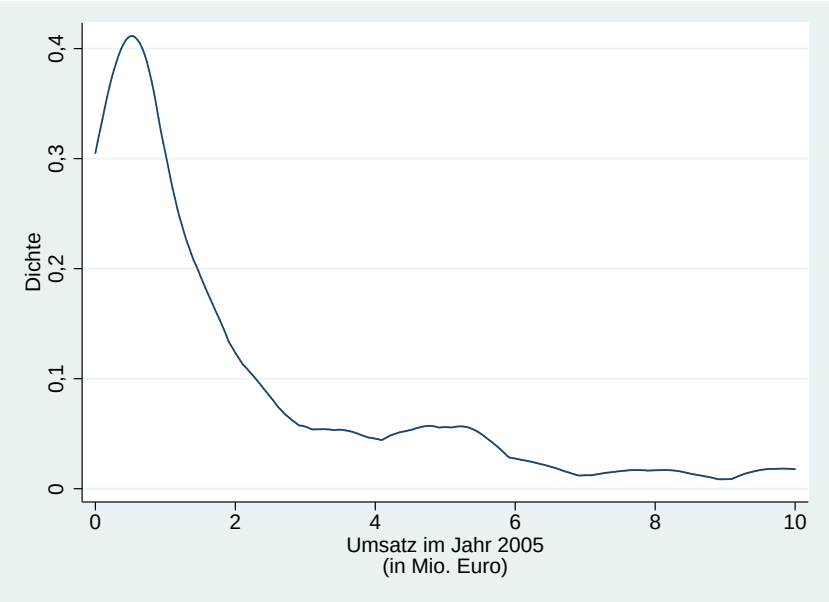


Anz. Beob. 782; Median 20; Mittelwert 135; Std. Abw. 860

Abbildung 5.1: Anzahl der Mitarbeiter

Über ihre Umsätze aus dem Jahr 2005 gaben 662 Teilnehmer Auskunft, davon setzte jeder dritte weniger als 500.000 Euro pro Jahr um, 25 Unternehmen hatten sogar nur Umsätze von maximal 10.000 Euro. Weiterhin zeigt Abbildung 5.2, dass mehr als die Hälfte der Unternehmen im Jahr 2005 Umsätze von mindestens einer Million Euro zu vermelden hatten, bei jedem vierten Unternehmen lag der Wert sogar über fünf Millionen. Auch hier sorgen einzelne Unternehmen für eine große Abweichung zwischen Mittelwert und Median, da sie mehr als eine Milliarde Umsatz angegeben haben, der Maximalwert lag bei 8,3 Milliarden Euro. Während die Umsätze am Median bei 1,21 Millionen Euro liegen, beträgt der Mittelwert bedingt durch vier Unternehmen mit mehr als einer Milliarde Euro Umsatz im Vorjahr der Befragung 46,2 Millionen Euro.

Die Daten für die in diesem Abschnitt abgebildeten Kerndichteschätzungen wurden aus Darstellungsgründen auf Unternehmen mit bis zu 200 Mitarbeitern sowie mit maximal 10 Millionen Euro Umsatz begrenzt, einen vollständigen Überblick über die Verteilungen gibt Tabelle B.1 in Anhang B.



Anz. Beob. 662; Med. 1,21 Mio.; MW 46,2 Mio.; Std. Abw. 446,7 Mio.

Abbildung 5.2: Umsatzzahlen im Jahr 2005 (in Mio. Euro)

Auch die Daten für das Streudiagramm zur Darstellung des Zusammenhangs zwischen der Größe des Personalbestands und dem Umsatz eines Unternehmens im Jahr 2005 wurden aus Gründen der Übersichtlichkeit um die Ausreißer bereinigt. Wie dem Diagramm in Abbildung 5.3 entnommen werden kann, unterliegt der Umsatz pro Mitarbeiter einer recht großen Varianz. Doch obwohl der Pro-Kopf-Umsatz ein breites Spektrum abdeckt, ballt sich fast die Hälfte der Unternehmen in einem Umsatzbereich zwischen 50.000 und 100.000 Euro je Mitarbeiter. Diese Beobachtung gilt auch für die Unternehmen in der dichten Punktwolke von bis zu 20 Mitarbeitern, die gemäß Abbildung 5.1 die Hälfte der betrachteten Betriebe ausmacht, dieses Detail kann in Abbildung B.7 im Anhang nachvollzogen werden.

Während entsprechend des Schaubilds einige Firmen enorme Umsätze mit geringem Personalaufwand erzielen, überrascht die relativ große Zahl jener Unternehmen, die nach eigenen Angaben keine oder nur geringe Umsätze in Relation zu ihrem Personalbestand erwirtschaften. Die Kerndichteschätzung in Abbildung 5.4 bestätigt den Eindruck, dass einige Betriebe eigentlich nicht in der Lage sein sollten, mit den realisierten Umsätzen ihre eigenen Personal-

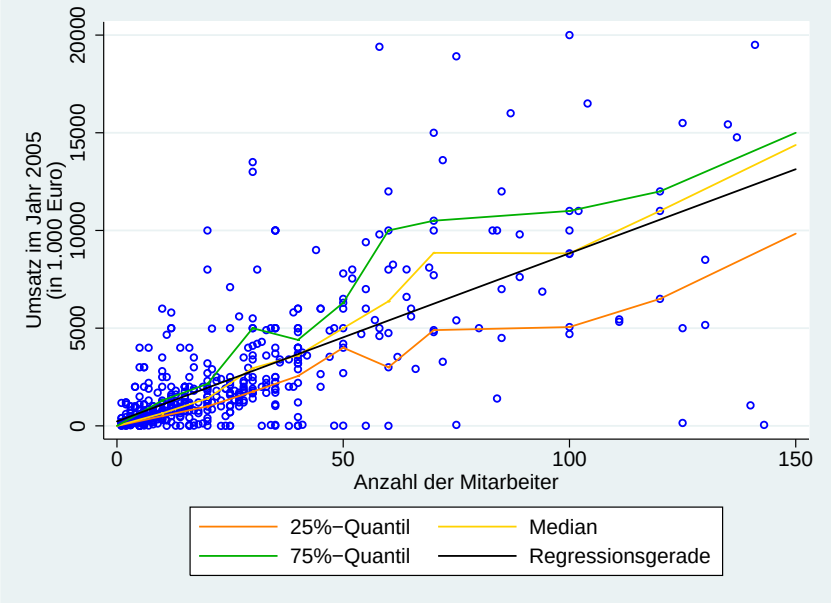
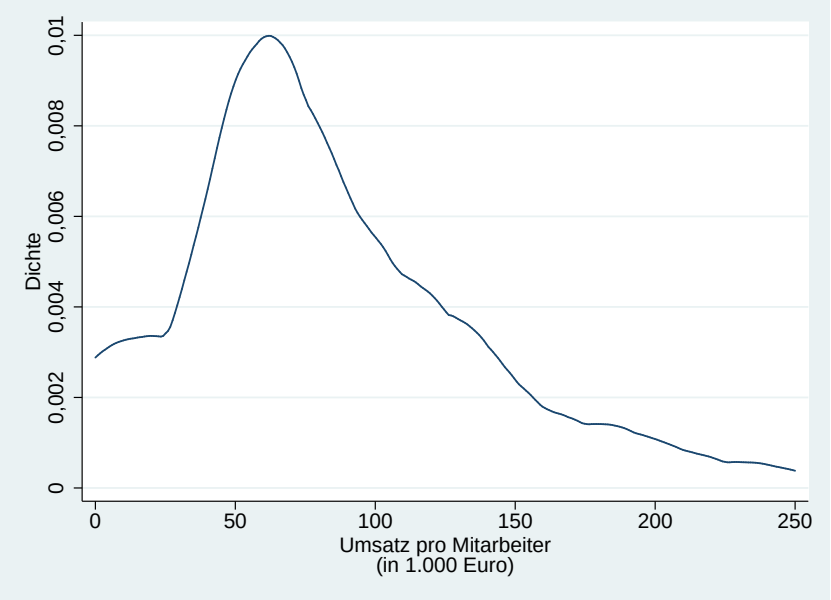


Abbildung 5.3: Streudiagramm für die Anzahl der Mitarbeiter und Umsatz

kosten zu decken. So liegt bei jedem fünften Unternehmen der Umsatz pro Mitarbeiter unter 50.000 Euro und es stellt sich die Frage, ob die Angaben zum Jahresumsatz nicht korrekt gemacht wurden, sei es bewusst oder versehentlich. Schließlich kann ein Unternehmen zumindest in der Marktwirtschaft nur dann dauerhaft existieren, wenn wenigstens mittel- und langfristig schwarze Zahlen geschrieben werden, hierfür muss jedoch mehr Umsatz erwirtschaftet werden, als zur reinen Deckung der Personalkosten nötig ist.

Dagegen sind in Bezug auf die Umsatzzahlen Ausreißer nach oben weniger kritisch zu betrachten, da hohe Umsätze nicht mit hohen Gewinnen gleichzusetzen sind, insbesondere wenn den hohen Erlösen ähnlich hohe Kosten gegenübergestellt werden müssen. Wird dieser Gedanke weiter verfolgt, so ergibt sich als möglicher Grund für diese niedrigen Werte, dass von einzelnen Unternehmen statt des Umsatzes der Gewinn angegeben worden ist, bei den Personalzahlen sind solche Missverständnisse hingegen nicht zu erwarten. Inwiefern die Umsatzzahlen daher zu verlässlichen bzw. signifikanten Ergebnissen führen, wird im Rahmen der Regressionen in Abschnitt 5.3.1 erörtert.



Anz. Beob. 638; Median 80.000; MW 647.000; Std. Abw. 6,58 Mio.

Abbildung 5.4: Umsatz pro Mitarbeiter im Jahr 2005 (in Tausend Euro)

5.1.2 Zahlungsbereitschaft für IT-Sicherheit

Die von den Unternehmen geäußerten Zahlungsbereitschaften für die Reduzierung der Bedrohung durch Schadprogramme sowie die Senkung des Anteils unerwünschter E-Mails sind in Tabelle 5.4 dargestellt. Auf eine grafische Wiedergabe der Verteilung der absoluten Zahlungsbereitschaften wurde an dieser Stelle aus Darstellungsgründen verzichtet, da beispielsweise bei einem Boxplot bedingt durch die deutlichen Ausreißer weder der untere *„Whisker“* noch der Interquartilsabstand erkennbar gewesen wäre.

WTP	**Malware**				**Spam**			
Quantil	30 %	50 %	70 %	90 %	30 %	50 %	70 %	90 %
Minimum	0	0	0	0	0	0	0	0
1%	0	0	0	10	0	0	0	0
5%	0	0	25	50	0	0	0	20
10%	0	0	60	100	0	0	30	50
25%	20	50	200	150	10	50	100	100
50%	200	200	700	500	100	100	300	400
75%	1.000	1.000	2.000	2.000	500	500	1.000	1.000
90%	5.000	5.000	10.000	10.000	1.200	2.000	5.000	4.000
95%	5.400	6.000	20.000	10.000	5.000	5.000	10.000	10.000
99%	50.000	10.000	75.000	30.000	20.000	20.000	30.000	30.000
Maximum	50.000	100.000	300.000	200.000	30.000	30.000	70.000	60.000
Anz. Beob.	161	163	220	221	168	163	217	216
Mittelwert	1.853	1.661	5121	3.311	835	1.078	2.126	2.108
Std. Abw.	6.978	8.051	22.941	14.356	3.015	3.301	6.808	6.210

Tabelle 5.4: Zahlungsbereitschaft für Reduzierung von Malware und Spam

Bei diesen Ausreißern nach oben handelt es sich jedoch nicht etwa um hochgegriffene Protestantworten, sondern bei näherer Betrachtung durchaus um realistische Angaben. Zur Untersuchung der hohen Werte wurde die absolute Zahlungsbereitschaft zum einen in Relation zum Jahresumsatz und zum anderen ins Verhältnis zur Mitarbeiterzahl gesetzt. Bei der Zahlungsbereitschaft für die Reduzierung der Malware-Gefahr lag immer nur höchstens einer dieser relativen Werte am Rand der Verteilung, in den meisten Fällen waren die Werte sogar sowohl bezogen auf den Umsatz als auch auf den Personalbestand nur noch im (oberen) Mittelfeld. In den wenigen Fällen, in denen die Zahlungsbereitschaften relativ zum Umsatz sehr hoch waren, fielen

sie bezogen auf die Mitarbeiterzahl weniger extrem aus, so dass umsatzschwächere Unternehmen trotzdem zu Investitionen für IT-Sicherheit bezogen auf die Größe der Personalbestands bereit waren. Ähnliches galt für den umgekehrten Fall, bei dem hohe Zahlungsbereitschaften pro Mitarbeiter in verhältnismäßig geringeren Werten relativ zum Umsatz resultierten. Demnach müssen Unternehmen, bei denen wenige Mitarbeiter hohe Umsätze erzielen, letzten Endes nur einen geringen Teil des Umsatzes in IT-Sicherheit investieren, um bei der Zahlungsbereitschaft pro Mitarbeiter einen Spitzenplatz zu erreichen.

Die Analyse der Zahlungsbereitschaft für die Verminderung des Spam-Aufkommens führte zu ähnlichen Ergebnissen, hier mussten jedoch drei Unternehmen genauer unter die Lupe genommen werden. Ein Unternehmen hatte in beiden relativen Zahlungsbereitschaften eine Spitzenposition inne, die beiden anderen hatten hingegen keinen Jahresumsatz angegeben und waren daher auf Basis dieses Wertes nicht vergleichbar. Das erstgenannte Unternehmen hatte mit 80 % Spam-Anteil am gesamten Mail-Aufkommen im Vergleich zu den anderen Beobachtungen ebenso einen hohen Wert angegeben wie beim Umsatzanteil durch E-Commerce. Zwar betrug der E-Commerce-Anteil absolut gesehen nur 20 %, er lag aber damit nur knapp unter dem 95 %-Quantil, so dass im Vergleich zu den anderen Unternehmen von einem sehr hohen Wert gesprochen werden kann und somit eine besondere Abhängigkeit von der Zuverlässigkeit der Informationstechnologie besteht.

Die beiden anderen Unternehmen waren zwar nur einer knapp unterdurchschnittlichen Spam-Belastung ausgesetzt, gaben jedoch beide an, in allen vorgegebenen Beobachtungszeiträumen, also in den Jahren 2005 und 2004 sowie davor jeweils Vorfälle durch Malware gehabt zu haben. Die von diesen Unternehmen geäußerten Zahlungsbereitschaften für die Reduzierung des Malware-Risikos waren ebenfalls relativ hoch ausgefallen, waren dort jedoch bei der Überprüfung der Ausreißer nicht auffällig gewesen. Eine hohe Zahlungsbereitschaft für die Bekämpfung von Spam, deren Verbreitung schon zum damaligen Zeitpunkt in Verbindung mit Botnetzen stand, ist daher nachvollziehbar. Insofern konnten die hohen Angaben zur Zahlungsbereitschaft in der Regressionsanalyse vollständig berücksichtigt werden und mussten nicht unter dem Verdacht der Protestantwort ausgefiltert werden.

Obwohl bei Zahlungsbereitschaften von null im Normalfall von Protestantworten ausgegangen wird, welche dann nicht in die Regression einfließen, wurden die Nullen in der vorliegenden Arbeit etwas differenzierter betrachtet. Unter der bereits geäußerten Annahme, dass einigen Befragten eine Reduzierung um 30 % oder 50 % nicht ausreicht und sie daher eine Zahlungsbereitschaft von null äußern, wurden Nullen genau dann nicht als Protestantwort angesehen, wenn gleichzeitig für die Reduzierung um eine höhere Quote eine valide Zahlungsbereitschaft angegeben worden war. Auf diese Weise wurden bei drei der vier Wertepaare nur wenige Protest-Nullen ausgefiltert, besonders viele Nullen als Paare gab es laut Tabelle 5.5 bei der Senkung des Spam-Anteils um 30 % bzw. 70 %.

	Malware		**Spam**	
	30 / 70 %	50 / 90 %	30 / 70 %	50 / 90 %
Protest-Nullen	3	2	11	6
gleiche Werte	4	4	10	4
entfernte Beob.	7	6	21	10

Tabelle 5.5: Protestantworten und gleiche Werte bei Zahlungsbereitschaften

Üblicherweise werden bei der Anwendung der CVM auch Antworten ausgefiltert, wenn davon ausgegangen werden muss, dass ein Proband die Frage nicht richtig verstanden hat. In der vorliegenden Studie wurde angenommen, dass dieser Fall zutrifft, wenn die Antworten für beide Reduzierungsanteile gleich groß waren, also beispielsweise für die Senkung des Malware-Aufkommens um 50 % die gleiche Zahlungsbereitschaft geäußert worden war wie für 90 %. Bei den zu äußernden Zahlungsbereitschaften trat dieser Effekt ähnlich wie bei den Protestantworten bei drei Wertepaaren nur selten auf, bei der Vermeidung von 30 % bzw. 70 % Spam zeigte sich jedoch wieder eine Konzentration der widersprüchlichen Antworten.

Während bei drei der vier Wertepaare jeweils insgesamt nur zwischen sechs und zehn Antworten entfernt werden mussten, waren bei den Antworten zur geringen Senkung des Anteils an Spam 21 Beobachtungen nicht verwertbar. Dieses geballte Auftreten nicht valider Antworten lässt den Schluss

zu, dass sogar eine Reduzierung des Spam-Anteils um 70 % von vielen Teilnehmern der Studie als nicht ausreichend erachtet worden war. Von den elf Unternehmen, welche für die Spam-Vermeidung um 70 % kein Geld bezahlen würden, hatten zehn vernünftige Werte bei der Zahlungsbereitschaft für die Reduzierung des Malware-Aufkommens angegeben. Obwohl neun dieser Teilnehmer einen Spam-Anteil von maximal 10 % zu beklagen hatten und somit eine Zahlungs-Nicht-Bereitschaft durchaus nachvollziehbar war, wurden die Antworten als mögliche Protest-Nullen dennoch nicht weiter berücksichtigt. Insgesamt hat bei den Fragen zur Zahlungsbereitschaft nur ein Unternehmen ausschließlich Nullen zu Protokoll gegeben, in allen anderen Fällen war zumindest bei der alternativen Antwortkategorie eine (positive) Zahlungsbereitschaft geäußert worden.

WTP	**Malware**				**Spam**			
Quantil	30 %	50 %	70 %	90 %	30 %	50 %	70 %	90 %
Minimum	0	0	10	10	0	0	1	2
1%	0	0	10	15	0	0	10	5
5%	0	0	50	50	0	0	30	50
10%	0	0	100	100	0	0	60	100
25%	25	50	200	150	20	50	120	100
50%	200	200	800	500	100	100	400	400
75%	1.000	1.000	2.000	2.000	500	500	1.000	1.000
90%	3.000	5.000	7.200	10.000	1.200	2.000	5.000	4.000
95%	5.400	6.000	12.600	10.000	5.000	5.000	10.000	10.000
99%	50.000	10.000	60.000	30.000	20.000	10.000	50.000	30.000
Maximum	50.000	100.000	300.000	200.000	30.000	30.000	70.000	60.000
Anz. Beob.	154	157	213	214	147	153	196	205
Mittelwert	1.580	1.301	3.924	2.613	875	1.035	2.172	1.953
Std. Abw.	5.903	4.949	13.041	8.926	3.242	2.867	7.016	5.308

Tabelle 5.6: Absolute Zahlungsbereitschaft nach Datenbereinigung

Die Verteilung der absoluten Zahlungsbereitschaften nach der Entfernung potentieller Protestantworten sowie widersprüchlicher Werte geht aus Tabelle 5.6 hervor. Für jede Frage lagen bei den niedrigen Werten zwischen 147 und 157 Antworten vor, für die hohen Werte zwischen 196 und 214 Antworten, diese Differenz begründet sich darin, dass viele Unternehmen nur eine Zahlungsbereitschaft für die besseren Werte angegeben hatten. Diese systematisch fehlenden Angaben nähren die Vermutung, dass für diese Beobachtungen bei den niedrigen Werten implizit von einer Zahlungsbereitschaft von

0 Euro ausgegangen werden kann. Da diese Werte allerdings nicht explizit geäußert worden waren, kann die Annahme nicht bestätigt werden, so dass an dieser Stelle keine Anpassung der Daten vorgenommen wurde, um die Ergebnisse nicht zu verzerren.

Die Kerndichteschätzungen der relativen Zahlungsbereitschaften sind in den Abbildungen 5.5 bis 5.8 dargestellt, auf jeder Seite wird eine der beiden Fragestellungen im Verhältnis zur Mitarbeiterzahl oder zur Höhe des Jahresumsatzes behandelt. Dabei sind die Grafiken jeweils so angeordnet, dass auf einer Seite die Verteilungen von 30 % bis 90 % von oben nach unten angeordnet sind. Die linke Spalte zeigt die Antworten für den Fall, dass die Frage zuerst gestellt wurde, dementsprechend finden sich in der rechten Spalte die Antworten auf die an zweiter Position gestellten Fragen. Den Schätzungen liegen dabei bereits die von Protestantworten und anderen Fehlerquellen bereinigten Antworten aus Tabelle 5.6 zugrunde. Die entsprechenden Streudiagramme finden sich in Abbildungen B.1 bis B.4 im Anhang.

Bei der Betrachung der Abbildungen fallen mehrere Eigenschaften der Verteilungen auf, manche davon sind recht offensichtlich und auch wenig überraschend. So sind die Zahlungsbereitschaften für die Reduzierung des Malware-Aufkommens durchweg höher als jene für die Senkung des Spam-Anteils, was die eingangs geäußerte Annahme bestätigt, dass der Bedrohung durch Schadprogramme ein höheres Schadens- und damit Kostenpotential zugestanden wird als der Belästigung durch unerwünschte E-Mails. Zwar teilten einzelne Unternehmen diese Meinung nicht und haben für die Bekämpfung von Spam-Mails höhere Zahlungsbereitschaften geäußert als für den Schutz vor Schadprogrammen, diese Ausnahmen machen jedoch weniger als sieben Prozent jener Unternehmen aus, die in der Umfrage Angaben zur Zahlungsbereitschaft gemacht haben. Darüber hinaus hatte fast die Hälfte dieser Abweichler noch nie Vorfälle durch Malware zu vermelden, jedes dritte hingegen mit mindestens 50 % Spam-Anteil zu kämpfen, auf jedes sechste Unternehmen trafen beide Eigenschaften zu. Somit lässt sich die Abweichung vom erwarteten Verhalten bei 19 der 33 Unternehmen durch die jeweils spezifische Bedrohungssituation der IT-Sicherheit erklären.

Beim direkten Vergleich der in einem Fragebogen abgefragten Wertepaare zur Reduzierung einer der beiden Gefahren aus dem Internet liegen die

Zahlungsbereitschaften für das größere Verbesserungspotential erwartungsgemäß deutlich höher. Dieses Verhalten ist fast allen Fällen beim Vergleich der ersten und dritten bzw. zweiten und vierten Abbildung einer jeden Spalte recht offensichtlich. Auch entsteht teilweise der Eindruck, dass sich die Verteilungsfunktionen für die Reduzierung von 30 % bis 90 % über die Beobachtungsgruppen hinweg in der gleichen Sequencing-Gruppe, also innerhalb einer Spalte leicht nach rechts verschieben, dieser Effekt kann beispielsweise anhand der Schaubilder in Abbildung 5.6 nachvollzogen werden.

Über möglicherweise auftretende Sequencing-Effekte lassen sich anhand der Abbildungen noch keine verbindlichen Aussagen treffen, so scheinen beispielsweise die geäußerten Zahlungsbereitschaften für die Reduzierung des Spam-Volumens bei 70 % und 90 % höher zu sein, wenn die Frage an zweiter Position gestellt worden war. Dies wäre der Vermutung zuträglich, dass die zuvor erfragte Zahlungsbereitschaft für Malware die Probanden bezüglich des Gefahrenpotentials im Internet sensibilisiert haben könnte. Bei der Bekämpfung von Schadprogrammen tritt dieses Antwortverhalten ebenfalls teilweise auf und entspräche somit dem ab Seite 62 geschilderten Beispiels, nach einem bereits geäußerten Wert in der ersten Frage zum zweiten Wert eine Steigerung für ein als wertvoller erachtetes Gut kundtun zu müssen. Vereinzelt zeigt sich aber auch bei beiden Problemstellungen die typischerweise auftretende Form des Sequencing, bei welcher die Antworten auf die an zweiter Stelle positionierten Fragen infolge von Einkommenseffekten niedriger ausfallen. Aufschluss über möglicherweise auftretende verschiedene Formen des Sequencing können daher erst die Regressionen in Abschnitt 5.3.1 geben.

5.1.3 Vorfälle durch Malware und Spam-Situation

Ein im Vorfeld der Erhebung als problematisch erachtetes Thema war die Frage nach durch Malware verursachten Vorfällen in den Unternehmen. Aus diesem Grund war diese Frage beim Design des Fragebogens an das Ende desselben gelegt und erst an vorletzter Position gestellt worden. Überraschend hoch war die Auskunftsbereitschaft der Unternehmen bei der „Gretchenfrage“, 807 der 844 befragten Unternehmen äußerten sich zu dem heiklen Thema.

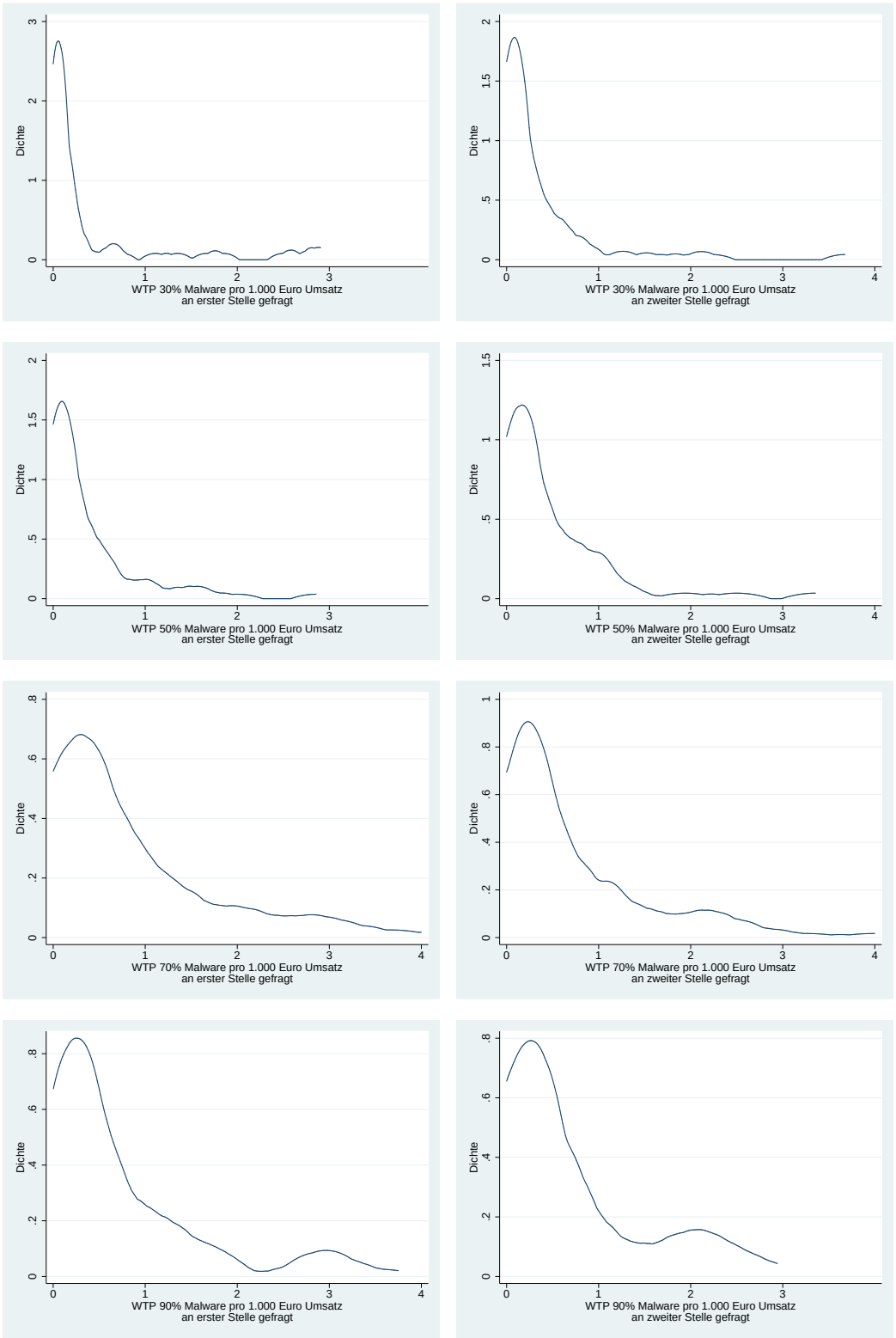


Abbildung 5.5: Zahlungsbereitschaft für Malware pro 1.000 Euro Umsatz

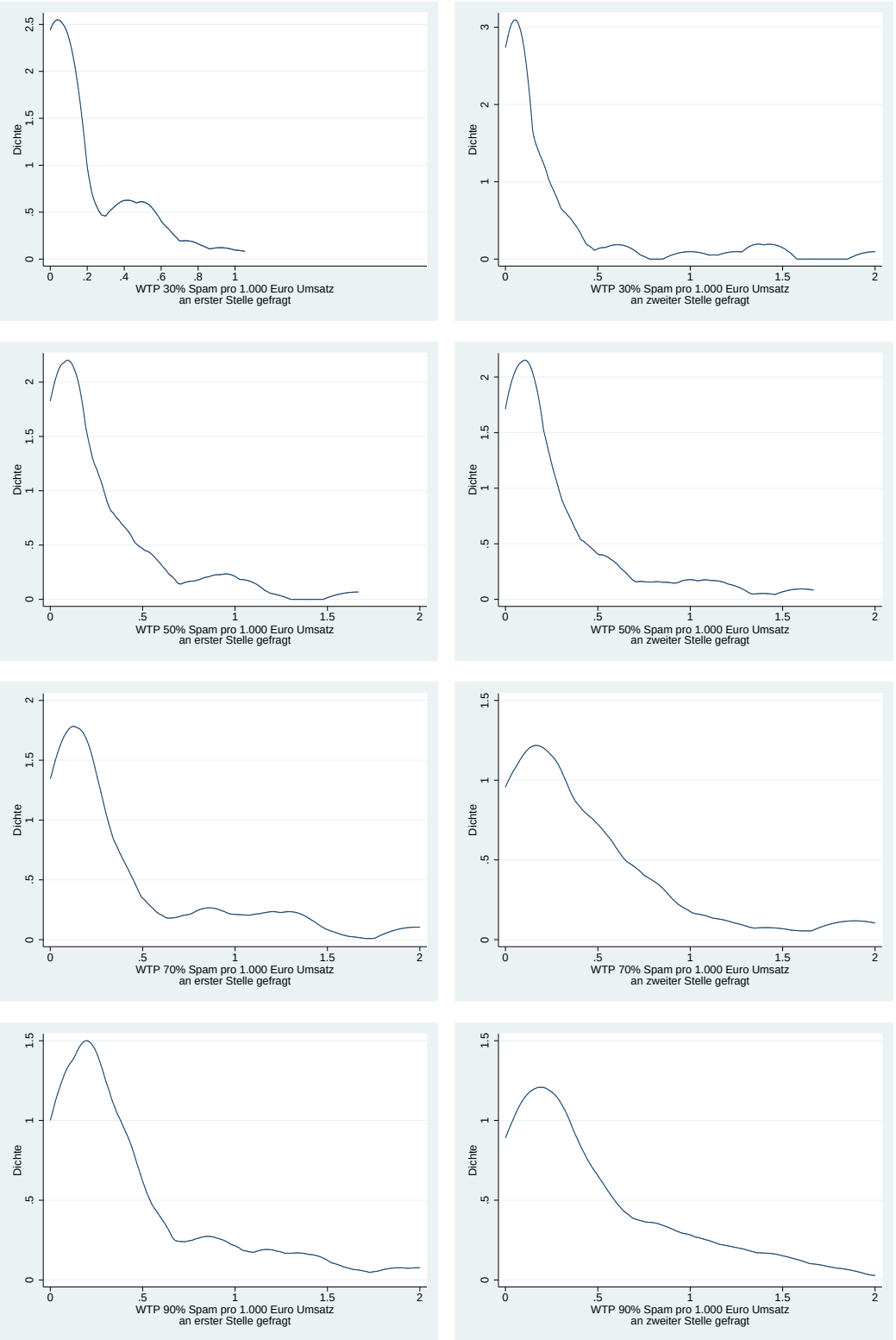


Abbildung 5.6: Zahlungsbereitschaft für Spam pro 1.000 Euro Umsatz

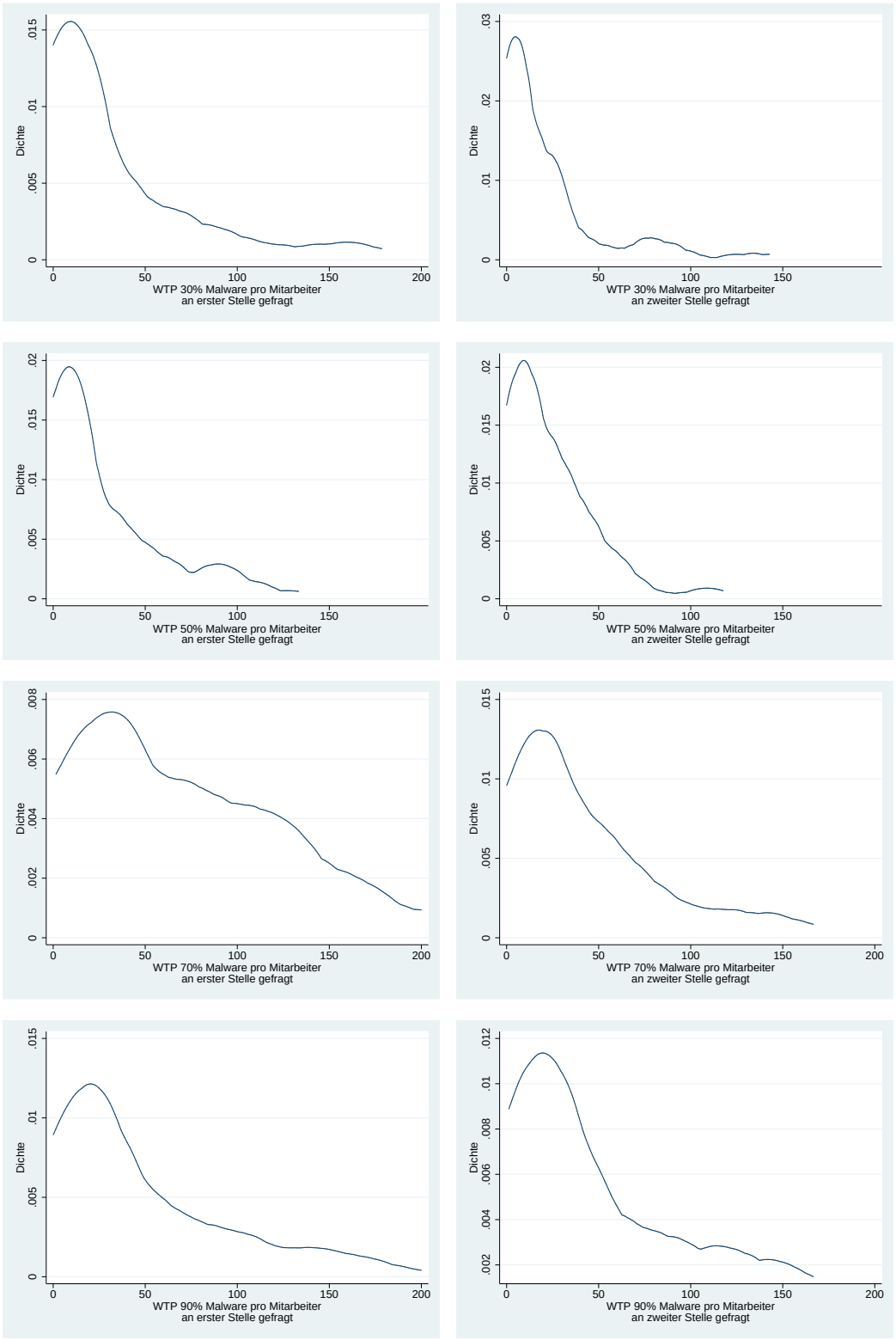


Abbildung 5.7: Zahlungsbereitschaft für Malware pro Mitarbeiter

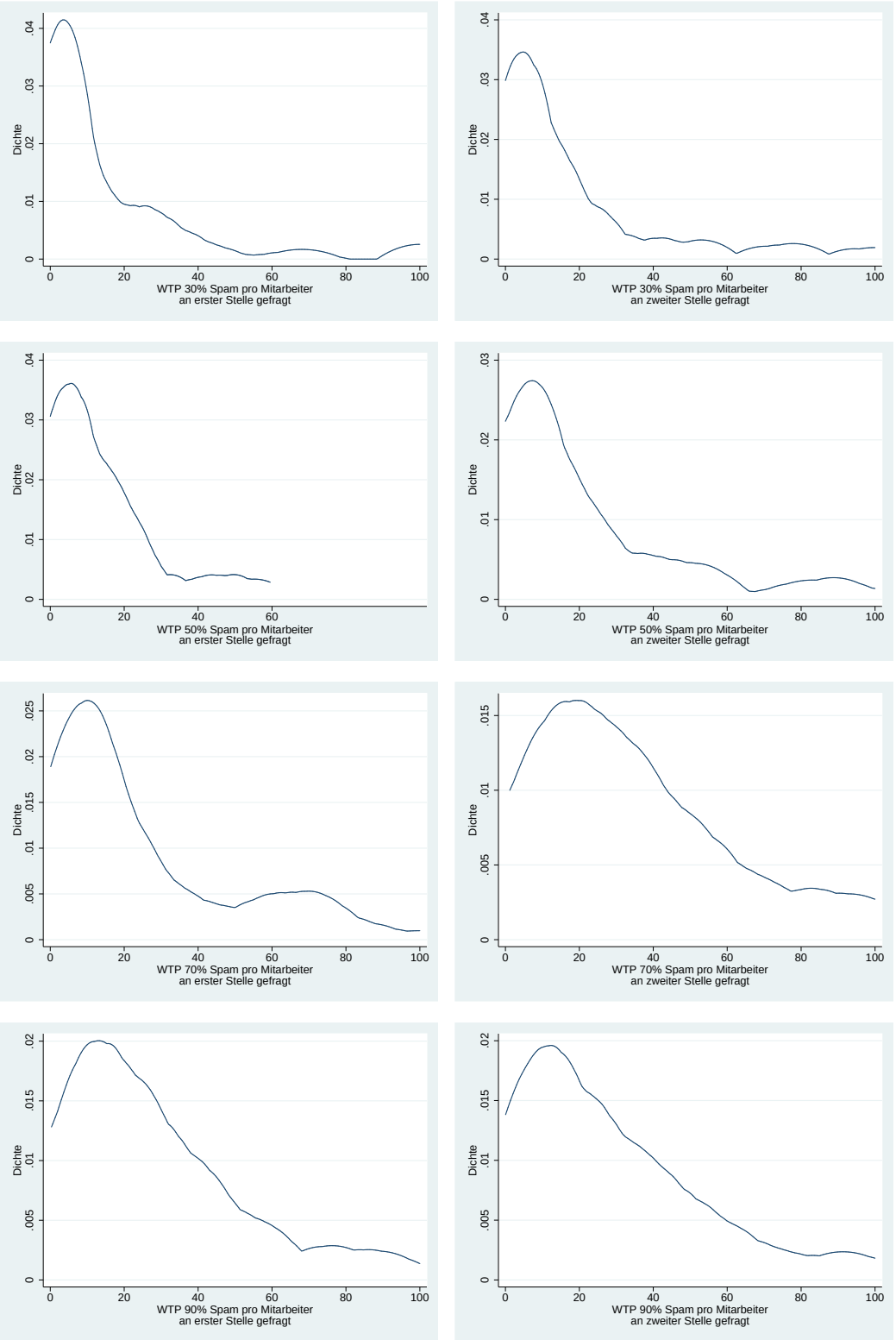


Abbildung 5.8: Zahlungsbereitschaft für Spam pro Mitarbeiter

Fast die Hälfte der Teilnehmer, welche auf die Frage geantwortet haben, gab gemäß Tabelle 5.7 an, noch nie Vorfälle durch Schadprogramme gehabt zu haben. Dabei kann angenommen werden, dass es sich in diesen Fällen nicht um unentdeckte Infektionen gehandelt haben dürfte, da diese über einen längeren Zeitraum entdeckt worden wären. Vorausgesetzt, dass die Unternehmen bei dieser Frage wahrheitsgemäß geantwortet haben, liegt die Wahrscheinlichkeit für Vorfälle durch Schadprogramme damit bei den IKT-intensiven Dienstleistern recht niedrig.[3] Dieses geringe Malware-Risiko der Branchenvertreter ließe sich dann durch die fachliche Nähe zur Problematik sowie das möglicherweise daraus resultierende größere Gefahren-Bewusstsein begründen.

Zeitraum	Anz. Antw.	Zeitraum	Anz. Antw.
vor 2004	225	keine Vorfälle	396
im Jahr 2004	206	in den Jahren 2004 und 2005	127
im Jahr 2005	212	in allen drei Zeiträumen	83

Tabelle 5.7: Vorfälle durch Schadprogramme

Vorgreifend auf die Frage zum IT-Outsourcing kann hier noch erwähnt werden, dass fast 60 % der Unternehmen keine IT-Aufgaben ausgelagert haben. Bei diesen Firmen liegt der Anteil ohne Probleme mit Schadprogrammen bei 51 % und damit etwas höher als bei komplettem oder teilweisem Outsourcing (45 - 46 %). Dies lässt sich darauf zurückführen, dass durch die (teilweise) Abtretung der Verantwortung für die IT auch die Wahrnehmung von Problemen mit Malware „ausgelagert“ wird.

Unternehmen, die sich bei Fragen der IT-Sicherheit von externer Seite beraten lassen, haben dagegen nur in 45 % der Fälle angegeben, Malware-frei zu sein, gegenüber 54 % bei Unternehmen ohne Beratung von Dritten. Demnach lassen sich Unternehmen mit Malware-Problemen zumindest nach einem Vorfall eher von Experten für IT-Sicherheit beraten.

[3] Bei einer <kes>-Studie (2006a) hatten zum Vergleich 72 % der Teilnehmer angegeben, allein im Jahr 2005 mindestens einen Vorfall durch Malware gehabt zu haben.

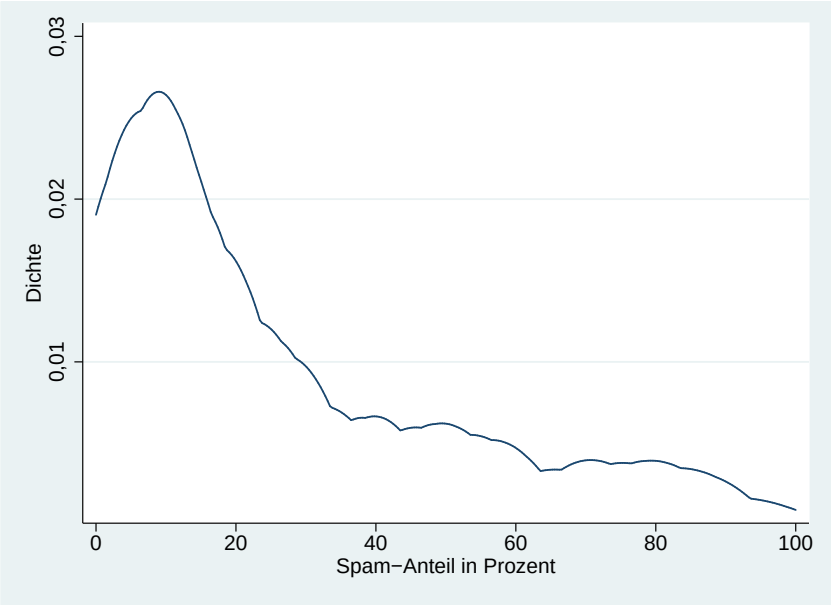
Von den verbleibenden 411 Firmen hatte ungefähr die Hälfte Malware-Probleme im Jahr 2005, ebenso wie im Jahr 2004, auch vor dem Jahr 2004 hatte jedes zweite der Unternehmen Vorfälle zu beklagen. Mit 127 Betrieben hatte immerhin mehr als jeder vierte Teilnehmer mit Malware-Befall Vorfälle in den Jahren 2004 und 2005 zu vermelden. Besonders hart traf es 83 Unternehmen, die nach eigenen Angaben sowohl in den Jahren 2005 und 2004 als auch davor Probleme mit Viren, Würmern und Trojanern gehabt haben. Die Angaben zu Vorfällen in den Jahren 2004 und 2005 sind mit 0,47 (signifikant) korreliert, der Zeitraum vor 2004 weist jedoch mit Werten unter 0,3 keine Korrelation zu diesen beiden Jahren auf.

Quantil	Anteil	Quantil	Anteil	Quantil	Anteil
Min.	0	25 %	5	90 %	70
5 %	1	50 %	15	95 %	80
10 %	2	75 %	40	Max.	100
Anz. Beob.	727	Mittelwert	25,3	Std. Abw.	25,0

Tabelle 5.8: Spam-Anteil am täglichen E-Mail-Aufkommen (in Prozent)

Ein weiterer Faktor, von welchem vermutet werden konnte, dass er einen direkten Einfluss auf die zu äußernden Zahlungsbereitschaften haben könnte, war der Anteil der Spam-Mails am gesamten E-Mail-Aufkommen eines Unternehmens, zu dieser Frage hatten 727 Unternehmen Angaben gemacht. Beim Vergleich mit dem nach Ironport (2006) damals üblichen Spam-Aufkommen von 67 % bis 76 %[4] fällt auf, dass die Belastung der IKT-intensiven Dienstleister erheblich geringer ausfällt. Der Mittelwert ist aufgrund der teilweise hohen Spam-Quoten bei 25 % angesiedelt, der Median hingegen liegt bei 15 % unerwünschter E-Mails am täglichen Mail-Aufkommen. Ein Viertel der Teilnehmer hatte sogar einen Spam-Anteil von maximal 5 % angegeben, während nur jedes fünfte Unternehmen mehr Spam als erwünschte E-Mails empfängt. Bei einer ungefähr zeitgleich durchgeführten Studie der BSI-Zeitschrift <kes> (2006b) lag der Median bei 33 % und damit deutlich

[4]Dieser Wert hängt davon ab, ob die auf Seite 20 vorgestellten *Misdirected Bounces* als Spam erachtet werden.



Anz. Beob. 727; Median 15 %; Mittelwert 25,3 %; Std. Abw. 25,0 %

Abbildung 5.9: Kerndichteschätzung des Spam-Aufkommens

höher, hier verfügten vier von fünf teilnehmenden Unternehmen und Institutionen über eine serverseitige Spam-Abwehr, drei Fünftel sogar über Maßnahmen auf den Clients.

Ob und welche Filtermaßnahmen zum Einsatz kommen, wurde bei der ZEW-Umfrage nicht gefragt, so dass nicht ausgeschlossen werden kann, dass einzelne Unternehmen ihre Angaben zur Spam-Quote am Mail-Aufkommen auf Basis des Anteils nach der Spam-Filterung gemacht haben. Dieser Gedanke wird in Abschnitt 5.3.3 bei der Untersuchung der Einflussfaktoren auf den Spam-Anteil aufgegriffen.

5.1.4 Weitere Einflussfaktoren

Die folgenden Seiten geben einen kurzen Überblick über all jene Variablen, welche abgesehen vom zuerst betrachteten Anteil der PC-Arbeitsplätze bei den Regressionen in Abschnitt 5.3 einen signifikanten Einfluss auf die geschätzten Koeffizienten nehmen. Die entsprechenden Abbildungen dazu sind bei Bedarf Anhang B ab Seite 197 zu entnehmen.

Anteil der PC-Arbeitsplätze

Computerarbeitsplätze spielen in der IKT-Branche erwartungsgemäß eine große Rolle, so haben laut Abbildung B.8 42 % der Unternehmen angegeben, dass alle ihre Mitarbeiter mit einem Rechner ausgestattet seien, bei der Hälfte der Teilnehmer lag der Anteil der Computerarbeitsplätze bei mindestens 95 %. Bei drei von fünf befragten Firmen verfügten noch mindestens 90 % aller Mitarbeiter über einen Arbeitsplatz mit Computer, nur bei jedem fünften Betrieb lag der Anteil der Mitarbeiter ohne Rechner über dem Anteil mit Computerausstattung. Sowohl in der ungewichteten als auch in der gewichteten Stichprobe lag der Anteil der Arbeitsplätze mit einem PC, Laptop, Terminal oder einer Workstation im Mittel bei 77 %. Demnach war (bei der gewichteten Stichprobe) der Anteil der Beschäftigten, welche den überwiegenden Anteil ihrer Arbeit an einem Computer erledigen, nach ungefähr 74 % im Jahr 2004 und etwa 78 % im Jahr 2005 geringfügig zurückgegangen [V05].

E-Commerce

Der elektronische Handel scheint auch in den Branchen der IKT-nahen Dienstleister noch nicht mehrheitsfähig zu sein, zumindest haben 61 % der befragten Unternehmen angegeben, nicht als Anbieter auf dem „Virtuellen Marktplatz“ aufzutreten. Immerhin 31 % der Teilnehmer bieten demnach anderen Unternehmen an, bei ihnen Bestellungen über das Internet aufzugeben, ein Service, den nur 19 % ihren Endkunden zur Verfügung stellen, nur jedes zehnte Unternehmen bietet sein E-Commerce-Angebot für all seine Kunden an. Zum Vergleich steigt bei der Gewichtung für den „ZEW Branchenreport“ der Anteil der Firmen, welche ihre Endkunden per E-Commerce bestellen lassen, sprunghaft auf 51 % an, nachdem gemäß Vanberg (2005) im Vorjahr dieser Anteil von 40 % auf 32 % gefallen war. Dieser Ausreißer bei einer Entwicklung, der eigentlich (mathematische) Monotonie unterstellt werden kann, lässt sich durch die zu starke Gewichtung schwach besetzter Beobachtungsklassen erklären, da wie bereits erwähnt in der vorliegenden Studie drei der neun Wirtschaftszweige über insgesamt sechs Beobachtungen verfügen.

Bedingt durch das von nur knapp 40 % der befragten Unternehmen zur Verfügung gestellte Angebot der Bestellungsaufnahme über das Internet liegt

der mittlere Umsatzanteil des E-Commerce insgesamt bei knapp 5 %, eine Verteilung der Umsatzanteile geht aus Abbildung B.9 hervor. Werden hingegen nur die Unternehmen betrachtet, die nach eigenen Angaben ihre Dienstleistungen über den elektronischen Marktplatz anbieten, beträgt dieser Anteil am Gesamtumsatz im Mittel immerhin 12 %, während der Median bei 5 % liegt. Insgesamt liegt der Anteil der Betriebe, die mehr als die Hälfte ihres Umsatzes mit Online-Handel erwirtschaften, bei 2 %, bezogen auf die Anbieter von E-Commerce verdreifacht sich dieser Anteil. Dagegen schätzten insgesamt drei Viertel der Firmen ihren Umsatzanteil durch das Internet-Angebot auf 0 %, obwohl nur gut 60 % angegeben hatten, keine Bestellungen über das Internet anzunehmen, so dass etwa 14 % trotz E-Commerce-Angebot damit keine Umsätze realisieren. Die Nutzung der E-Commerce-Angebote Anderer erfreut sich hingegen größerer Beliebtheit, hier gaben 70 % der teilnehmenden Unternehmen an, dass diese Möglichkeit, Bestellungen aufzugeben, von ihnen genutzt würde.

Weiterbildung und Aufklärung der Mitarbeiter

Auf die Frage, ob und inwiefern sie ihren Mitarbeitern eine Weiterbildung im Bereich IT-Sicherheit ermöglichten oder sie zumindest über mögliche Gefahren aus dem Internet aufklärten, haben 782 Unternehmen Auskunft erteilt. Demnach bekommen die Administratoren bei knapp der Hälfte der Unternehmen (382) die Chance zur Weiterbildung, immerhin fast jeder dritte Studienteilnehmer (230) ermöglicht diese Fortbildungsmaßnahmen sogar Mitarbeitern, die nicht im Bereich der IT-Administration tätig sind. Bei 62 % der Firmen (487) werden die Anwender zumindest über Gefahren aufgeklärt, die im Internet lauern, mit 125 Beobachtungen hat nur jedes sechste Unternehmen angegeben, dass es seinen Mitarbeitern weder eine Weiterbildung noch Aufklärung in diesem sensiblen Bereich zukommen ließ.

IT-Beratung und IT-Outsourcing

Bei der Administration des IT-Bereichs verlassen sich 60 % der Firmen auf ihre eigenen Fähigkeiten, 480 der 802 Antworten verneinten ein Outsourcing der IT-Administration. Mit 201 Unternehmen hat hingegen ein Viertel

der Antwortenden angegeben, einen Teil der Administration an externe Unternehmen ausgelagert zu haben, 121 Teilnehmer haben die Administration ihres IT-Bereichs sogar komplett in fremde Hände gegeben.

Bei der Beratung zu Fragen der IT-Sicherheit zeichnet sich dagegen eine klare Mehrheit für die Nutzung von externer Hilfe ab, fast zwei Drittel der Unternehmen ziehen Außenstehende zurate, um sich unterstützen zu lassen. Dagegen haben 294 von 800 Unternehmen angegeben, auch bei der IT-Sicherheit keine Beratung durch Dritte wahrzunehmen.

Budget-Anteile für IT-Sicherheit

Die Auswertung der Frage nach dem Anteil für IT-Sicherheit am IT-Budget ergab bei den (bundesweiten) Vertretern der IKT-Dienstleister ähnliche Ergebnisse wie die (in Baden-Württemberg durchgeführte) FAZIT-Umfrage (2005). Wie aus Abbildung B.10 ersichtlich ist, hat etwas weniger als die Hälfte der Unternehmen angegeben, zwischen einem und fünf Prozent des IT-Budgets in IT-Sicherheit zu investieren, bei ungefähr einem Achtel lag dieser Anteil zwischen sechs und zehn Prozent. Mit fünfzig Teilnehmern haben dagegen lediglich 6 % der Firmen angegeben, mehr als zehn Prozent ihrer IT-Ausgaben für die IT-Sicherheit aufzuwenden. Ungefähr jedes Vierte der befragten Unternehmen hat geäußert, dass es keine Angaben zum Anteil der IT-Sicherheit an seinem IT-Budget machen könne (oder wolle), weitere 9 % haben dies implizit getan, indem sie die Frage nicht beantwortet haben.

Abgesehen von kleineren Schwankungen entspricht die Verteilung der einzelnen Klassen dieser Studie ungefähr der Verteilung aus der FAZIT-Umfrage, einzige Ausnahme stellt die Antwortmöglichkeit von 0 % Budget-Anteil dar, welche in dieser Studie nicht angeboten worden war. Im Übrigen ist es durchaus möglich, dass bei der IKT-intensiven Dienstleistungsbranche die Budget-Anteile für die Informations- und Kommunikationstechnologie am Gesamtbudget höher sind, so dass die Anteile der IT-Sicherheit am Gesamtbudget relativ gesehen größer ausfallen.

5.2 Faktorenanalyse

Nach der deskriptiven Betrachtung der Variablen wurde eine Faktorenanalyse durchgeführt, um neben Zusammenhängen zwischen den Variablen, welche aus Korrelationsmatrizen hervorgehen, weitere Ähnlichkeiten und Abhängigkeiten unter den Variablen zu identifizieren. Da bei der Faktorenanalyse nicht die Untersuchung kausaler Zusammenhänge im Mittelpunkt stand, wurde die in Abschnitt 3.3.1 vorgestellte Hauptkomponentenanalyse zur Extraktion der Faktoren gewählt. Die Faktoren sollten also die betrachteten Variablen mit möglichst wenigen Faktoren darstellen und damit zur reinen Dimensionsreduktion dienen, um die Erkenntnisse aus der deskriptiven Analyse im Vorfeld der Regression zu erweitern.

5.2.1 Vorbereitung der Faktorenanalyse

Noch vor dem ersten Durchgang mussten die Daten speziell für die Faktorenanalyse aufbereitet werden, da Beobachtungen, für die in mindestens einer Variablen kein Wert angegeben ist, die also einen *„missing value“* besitzen, in der Analyse nicht berücksichtigt werden. Da nur bei 28 Beobachtungen alle Variablen mit einem Wert versehen waren, mussten die Missings bei binären (Indikator-)Variablen wenn möglich durch Nullen oder Einsen ersetzt werden. So wurden beispielsweise bei dem Fragenblock nach dem Anteil für IT-Sicherheit am IT-Budget Missings als „keine Angabe“ interpretiert, so dass bei den Antwortklassen mit Prozentangaben die Missings durch Nullen ersetzt wurden und die Missings bei „keine Angabe“ durch Einsen. Eine solche Interpretation war an dieser Stelle durchaus zulässig, da die Unternehmen die Frage durch die Nichtbeantwortung implizit mit „keine Angabe“ beantwortet hatten.

In diesem Zug wurden andere Variablen wie beispielsweise die Inanspruchnahme von IT-Beratung für die Faktorenanalyse gegenüber der ursprünglich beabsichtigten Auslegung der Fragestellung neu interpretiert, indem eine Eins aussagen sollte, das Unternehmen habe angegeben, es nutze diese Möglichkeit. Dadurch konnten die Missings durch Nullen ersetzt werden, welche dann verstanden werden konnten als „das Unternehmen hat nicht angegeben, dass es IT-Beratung nutzt“.

Nachdem alle Indikatorvariablen, bei denen ein Ersetzen der Missings interpretatorisch vertretbar war, überarbeitet waren, standen für die Analyse 393 Beobachtungen zur Verfügung. Der Grund für die relativ geringe Zahl an Beobachtungen – immerhin finden mit 47 % etwas weniger als die Hälfte der Unternehmen Eingang in die Analyse – liegt in der Sequencing-Variablen, für welche insgesamt nur 471 Beobachtungen vorlagen.[5] Diese Variable sollte in einer zweiten Analyse berücksichtigt werden, um mögliche, wenn auch eigentlich nicht zu erwartende Interdependenzen mit anderen Variablen bereits im Vorfeld der Regressionsanalysen feststellen zu können. Die genauere Untersuchung dieser Variablen, die eigentlich mit keiner der unternehmensspezifischen Variablen in Zusammenhang stehen sollte, sondern eigentlich einer zufälligen Verteilung unterliegen sollte, wird sich in Abschnitt 3.2.3 als durchaus berechtigt erweisen. In einer ersten Faktorenanalyse wurde die Sequencing-Variable nicht einbezogen, wodurch mit 623 Beobachtungen fast drei Viertel des Datensatzes betrachtet wurden.

Im ersten Durchgang wurden 33 Variablen in der Form, wie sie direkt aus dem Fragebogen hervorgegangen waren, berücksichtigt und durch 13 Faktoren abgebildet. Dabei wurden beispielsweise auch Variablen, welche eigentlich nur zur Umrechnung für die weitere Arbeit dienen sollten, bewusst in ihrer Ursprungsform einbezogen und erst im vierten Schritt auf die geplante Weise verwendet.

Zunächst wurden jedoch redundante (Kontroll-)Variablen entfernt, da sie erwartungsgemäß zusammen mit einer der anderen Variablen aus dem gleichen Fragenblock in einem Faktor abgebildet wurden. Üblicherweise wurden sie dabei mit der am stärksten mit Einsen besetzten Variablen mit umgekehrtem Vorzeichen und betragsmäßig ähnlicher Faktorladung zusammengefasst, so bildeten beispielsweise beim Anteil für IT-Sicherheit die Klassen „1-5 %“ und „keine Angabe“ einen eigenen Faktor. Generell wurde aus einer Gruppe

[5]Da die Sequencing-Variable anhand der gegebenen Antworten gesetzt wurde, beinhaltet sie lediglich die Information darüber, ob generell eine Zahlungsbereitschaft geäußert wurde. Sie wurde nicht verändert, wenn eine oder mehrere Zahlungsbereitschaften als Protestantworten entfernt wurden oder die Antwort als „nicht sinnvoll“ in der weiteren Untersuchung nicht berücksichtigt wurde, eine Bewertung der Antwortqualität fand in diesem Zusammenhang also nicht statt.

von Variablen eines Fragenblocks eine der beiden Variablen ausgeschlossen, die betragsmäßig am höchsten miteinander korreliert waren, die verbleibenden 26 Variablen wurden dann durch 12 Faktoren dargestellt.

Danach wurden die Administratoren mit unterschiedlichen Aufgabenbereichen in einer Variablen zusammengefasst, da sie mit weiteren Variablen in den ersten beiden Faktoren erklärt wurden, durch diese Substitution wurde die Zahl der Faktoren auf 11 reduziert. Im vierten Schritt wurden die Angaben zur Anzahl der Mitarbeiter mit IT-Ausbildung sowie der Administratoren umgerechnet, da die absoluten Zahlen wie vermutet mit der Anzahl an Mitarbeitern (signifikant) korreliert waren. Diese waren, wie bereits erwähnt, aufgrund der größeren Präzision der Angaben als absolute Werte erhoben worden und wurden im weiteren Verlauf der Untersuchung nur noch als relative Werte und somit unabhängig von der Unternehmensgröße betrachtet.

5.2.2 Ergebnisse der Faktorenanalysen

In der ersten endgültigen Faktorenanalyse wurden die 23 Variablen durch neun Faktoren abgebildet, die Entscheidung für die Anzahl der extrahierten Faktoren basierte hierbei auf dem Kaiser-Kriterium, wobei der 10. Faktor mit 0,990 nur knapp unter dem Grenzwert für das Kriterium liegt. Unter Berücksichtigung des Scree-Tests hätte die Entscheidung zwischen vier und elf Faktoren fallen müssen, wie die Differenzen in Tabelle 5.9 zeigen, es gibt also keine eindeutige Lösung bei der Verwendung dieses „schwachen“ Kriteriums. Mit einem Eigenwert von 2,503 erklärt der erste Faktor mehr als zehn Prozent der Gesamtvarianz, die ersten drei Faktoren bereits ungefähr ein Viertel. Die neun extrahierten Faktoren haben einen Erklärungsgehalt von 59,79 %, der Rest verteilt sich auf die übrigen 14 Faktoren.

Bei der Interpretation der rotierten Faktorladungsmatrix in Tabelle 5.10 fällt auf, dass bestimmte Variablen eindeutig einzelnen Faktoren zugeordnet werden können, andere wiederum verteilen ihre kleinen Faktorladungen auf bis zu drei verschiedene Faktoren. Dabei erweist sich die Zusammenstellung bestimmter Faktoren als wenig überraschend, aus diesem Grund wird auf den ersten Faktor (E-Commerce-Angebot), den vierten (Malware-Vorfälle), den

Erklärte Gesamtvarianz				
Faktor	**Eigenwert**	**Differenz**	**% der Varianz**	**Kumulierte %**
1	2,503	0,664	10,88	10,88
2	1,839	0,121	8,00	18,88
3	1,718	0,145	7,47	26,35
4	1,573	0,170	6,84	33,19
5	1,404	0,065	6,10	39,29
6	1,339	0,126	5,82	45,11
7	1,212	0,094	5,27	50,38
8	1,118	0,072	4,86	55,24
9	1,046	0,056	4,55	59,79
10	0,990	0,051	4,31	64,10
11	0,939	0,103	4,08	68,18
12	0,836	0,023	3,63	71,81
⋮	⋮	⋮	⋮	⋮

Tabelle 5.9: Erklärte Gesamtvarianz der Faktorenanalyse ohne Sequencing

neunten („Rolle der IT“) sowie die Kombination aus sechstem und siebtem Faktor (Anteil am IT-Budget) nicht näher eingegangen.

Obwohl auch die Verknüpfung von der Mitarbeiterzahl *(AnzMA)* und dem Jahresumsatz *(Ums2005)* im dritten Faktor so zu erwarten war, findet dieser hier Erwähnung, da die beiden Variablen für die kommenden Regressionen von grundlegender Bedeutung sind. Die beiden Variablen, deren Zusammenhang bereits durch die (signifikante) Korrelation von 0,649 offengelegt wurde, werden mit relativ hohen Faktorladungen und Kommunalitäten in einem Faktor abgebildet, welchem somit der Name „Unternehmensgröße“ zugewiesen werden kann. Wichtig ist diese starke Ähnlichkeit der Variablen vor Allem deshalb, weil im folgenden Abschnitt erhebliche Unterschiede zwischen den beiden aufgedeckt werden.

Die Faktoren zwei und fünf sind eng miteinander verknüpft und fokussieren auf „geschulte Admins“ und „Hilfe von außen“. Im zweiten Faktor gehen dabei Weiterbildungsmaßnahmen für Administratoren *(WBAdmin)* mit

Variable	1	2	3	4	5	6	7	8	9	Komm.
B2CAnt	0,7037									0,5578
B2Cb	0,6958									0,5079
B2Cc	0,6349									0,4783
B2B	0,5162							0,4304		0,5116
ITOutsrc		-0,8308								0,7289
WBAdmin		0,6006								0,5251
WBAnw		0,3839								0,3394
AntSumAI		0,3794								0,3883
ITOutsrcTeil					0,8204					0,7486
ITBerat		-0,4250			0,6783					0,6803
AntIT		0,3713			-0,3072				0,3929	0,4370
AnzMA			0,8920							0,8034
Ums2005			0,8842							0,7872
Mal2005				0,8153						0,6888
Mal2004				0,8234						0,6922
MalVor2004				0,4124				0,4016		0,4092
AufkAnw								0,6251		0,4981
AntSpam					-0,3391			0,3323		0,3965
RegWest							0,4803	-0,4430		0,5149
AntITS11plus							0,8164			0,7013
AntITS0105						-0,7986	-0,3345			0,7814
AntITS0610						0,8628				0,7982
PCAnt									0,8794	0,7770

Tabelle 5.10: Rotierte Faktorladungsmatrix ohne Sequencing

positivem Vorzeichen ein und stellen damit einen nachvollziehbaren Gegensatz zum kompletten Outsourcing der IT-Betreuung *(ITOutsrc)* dar, der Variablen mit der betragsmäßig höchsten Faktorladung dieser beiden Faktoren. Auch nehmen, den Faktorladungen nach zu urteilen, jene Unternehmen, die ihre Administratoren fortbilden (lassen), seltener IT-Beratung von externer Seite *(ITBerat)* in Anspruch. Der fünfte Faktor zeigt hingegen, dass das Nutzen von Beratungsangeboten im Bereich IT-Sicherheit häufig einhergeht mit einem teilweisen Auslagern der Administration der IT-Infrastruktur *(ITOutsrcTeil).* Ein geringer Anteil an IT-Fachkräften *(AntIT)* wird durch diesen Faktor teilweise miterklärt, hier ist aber der kleine Wert der Faktorladung zu beachten, so dass diese Variable ebenso wie die Weiterbildung der Anwender und der Anteil der Administratoren am Personalbestand durch die beiden Faktoren nur teilweise abgebildet wird.

Mit einer schwachen Faktorladung tritt der Spam-Anteil am E-Mail-Aufkommen *(AntSpam)* im Faktor „Hilfe von außen“ auf, das negative Vorzeichen lässt den Schluss zu, dass das Spam-Aufkommen bei den Unternehmen mit Beratung und teilweisem IT-Outsourcing geringer ist. Das gleiche Vorzeichen beim Anteil an IT-Fachpersonal und Spam-Anteil an E-Mails überrascht hingegen, insofern würde sich die Frage der Kausalität stellen, sofern ein Zusammenhang besteht. Tatsächlich ergäbe eine Regression einen signifikanten Einfluss, der marginale Effekt wäre allerdings vernachlässigbar gering, da bei einer Erhöhung des Anteils an IT-Fachkräften um ein Prozent der Anteil an Spam um 0,12 % steigen würde.[6]

Ebenfalls relativ schwach geladen zeigt sich die Spam-Variable im achten Faktor, welcher sich aus drei weiteren Variablen mit betragsmäßig kleinen Faktorladungen sowie der Unternehmensphilosophie, seine Anwender über Gefahren aus dem Internet aufzuklären *(AufkAnw),* zusammensetzt. Dabei ist ein Zusammenhang zwischen dem Nutzen von E-Commerce-Angeboten *(B2B),* Malware-Vorfällen vor 2004 *(MalVor2004),* dem Spam-Anteil und der Anwender-Aufklärung nachvollziehbar, ein Zusammenhang mit der regionalen Zuordnung der Unternehmen *(RegWest)* hingegen ist nicht offensichtlich.

[6]Bei einem Median von einem Prozent IT-Fachkräften entspräche dieser Wert zufällig der Spam-Erhöhung, welche die Hälfte der Unternehmen maximal zu erwarten hätte, bei zwei Dritteln der Unternehmen läge der Anstieg des Spam-Anteils unter einem Prozent.

Einerseits besteht bei erhöhtem Spam-Aufkommen sowie Malware-Befall in der Vergangenheit die Notwendigkeit, die Mitarbeiter zu informieren, andererseits birgt ein umfangreicher Umgang mit dem Internet, wie er aus Online-Bestellungen hervorgeht, ein Gefahrenpotential, vor dem gewarnt werden muss. Zu beachten sind bei diesem Faktor die relativ geringen Kommunalitäten für die Malware-Vorfälle vor 2004 sowie für den Anteil der Spam-Mails am Mail-Aufkommen. Die Werte von jeweils ca. 40 % deuten darauf hin, dass die beiden Variablen nur unzureichend durch die extrahierten Faktoren erklärt werden, dennoch ist ein Zusammenhang sowohl mit Blick auf die Zahlen als auch inhaltlich nicht von der Hand zu weisen.

Wird nun in einer weiteren Faktorenanalyse unter Einbeziehung der gleichen Beobachtungen die Kontrollvariable für das Sequencing *(MalVorSpam)* berücksichtigt, ändern sich die Ergebnisse nur geringfügig, sowohl in Bezug auf die einzelnen Faktorladungen als auch auf die Kommunalitäten. Bei dieser Faktorenanalyse werden unter Einbeziehung der Sequencing-Variablen die nunmehr 24 Variablen untersucht, die 393 Beobachtungen beinhalten nun nur noch jene Unternehmen, die eine Zahlungsbereitschaft geäußert haben, das Sequencing ist also in dieser Untersuchung ein implizites Filterkriterium. Gemäß dem Kaiser-Kriterium werden die 24 Variablen am Besten durch 11 Faktoren erklärt, bei der Bestimmung der optimalen Faktorenzahl über den Scree-Test wäre die Entscheidung zugunsten von 12 Faktoren gefallen, wie eindeutig aus den Differenzen der Eigenwerte in Tabelle 5.11 hervorgeht. Der Erklärungsgehalt der Faktoren unterliegt in beiden Analysen ungefähr der gleichen Verteilung, bedingt um die um eins größere Anzahl der Faktoren sind die kumulierten Werte mit einer Ausnahme im zweiten Fall geringfügig kleiner. Insgesamt erklären die extrahierten elf Faktoren in der zweiten Analyse mit 67,19 % mehr als zwei Drittel der Gesamtvarianz.

In der Faktorladungsmatrix haben sich die meisten Konstellationen gegenüber der ersten Faktorenanalyse nicht verändert, vor Allem bei Variablen mit hohen Faktorladungen ist alles beim Alten geblieben. Einige Variablen mit geringen Ladungswerten wurden hingegen neu zugeordnet, wie beispielsweise im zweiten Faktor zu sehen ist.

Vermutlich getrieben durch die kleinere Zahl der Beobachtungen nimmt der erste Faktor eine starke Position mit nur zwei Variablen ein, zum Vergleich setzen sich die nächsten Faktoren aus vier bzw. sechs Variablen zusammen.

Erklärte Gesamtvarianz				
Faktor	**Eigenwert**	**Differenz**	**% der Varianz**	**Kumulierte %**
1	2,534	0,464	10,56	10,56
2	2,070	0,383	8,62	19,18
3	1,687	0,149	7,03	26,21
4	1,538	0,112	6,41	32,62
5	1,426	0,088	5,94	38,56
6	1,338	0,101	5,57	44,13
7	1,237	0,064	5,15	49,29
8	1,172	0,096	4,89	54,17
9	1,077	0,038	4,49	58,66
10	1,039	0,030	4,33	62,99
11	1,009	0,051	4,20	67,19
12	0,958	0,114	3,99	71,18
13	0,844	0,010	3,52	74,70
14	0,834	0,052	3,48	78,17
⋮	⋮	⋮	⋮	⋮

Tabelle 5.11: Erklärte Gesamtvarianz der Faktorenanalyse mit Sequencing

Die Anzahl der Mitarbeiter weist dabei eine ebenso hohe Faktorladung auf wie der Umsatz aus dem Jahr 2005, und auch die Kommunalitäten der beiden Indikatoren der Unternehmensgröße liegen nahe 0,9.

Der zweite und vierte Faktor sind durch eine gemeinsame Variable im Zusammenhang zu sehen, der zweite Faktor fasst dabei das „E-Commerce-Angebot“ der Unternehmen zusammen. Obwohl die Angaben zum Online-Handel für Unternehmen *(B2Cb)* und Endkunden *(B2Cc)* sowie dem Umsatzanteil durch E-Commerce *(B2CAnt)* schwach miteinander korreliert sind, bilden sie hier einen gemeinsamen Faktor, dem mit umgekehrtem Vorzeichen Vorfälle durch Malware vor 2004 zugeordnet werden können. Dies lässt (ohne Unterstellung einer kausalen Richtung) die Vermutung zu, dass bei Unternehmen, für die E-Commerce eine wichtige Rolle spielt, in der Zeit vor 2004 weniger Probleme mit Schadprogrammen auftraten – oder diese zumindest nicht zugegeben werden.

Variable	1	2	3	4	5	6	7	8	9	10	11	Komm.
AnzMA	0,9358											0,8896
Ums2005	0,9319											0,8772
B2Cb		0,7718										0,6461
B2CAnt		0,7077										0,6467
B2Cc		0,5689										0,5020
MalVor2004		-0,3368		0,3260								0,4775
Mal2005				0,8382								0,7416
Mal2004				0,8254								0,7077
ITOutsrc			-0,8071									0,7208
WBAdmin			0,6335									0,5733
AntSumAI			0,3581					0,3635	-0,3277			0,4820
WBAnw			0,3721						0,3936			0,4595
AntIT			0,3472			-0,3538				0,3331	0,3663	0,5529
ITBerat			-0,4647			0,6073						0,6837
ITOutsrcTeil						0,8709						0,8070
AntITS0610					0,8605							0,8078
AntITS0105					-0,8167		-0,3432					0,8132
AntITS11plus							0,8198					0,7481
AufkAnw							0,5174					0,5837
AntSpam								0,6871				0,5885
B2B								0,6471				0,6146
RegWest									-0,7072			0,5790
PCAnt										0,9003		0,8172
MalVorSpam											0,8850	0,8061

Tabelle 5.12: Rotierte Faktorladungsmatrix mit Sequencing

Der Faktor „Malware-Vorfälle“ wird aus den mit starken Faktorladungen versehenen Vorfällen durch Schadprogramme in den Jahren 2005 *(Mal2005)* und 2004 *(Mal2004)* gebildet und durch Vorfälle vor dem Jahr 2004 ergänzt. Die Kommunalität von 47,8 % deutet darauf hin, dass die früheren Ereignisse auch hier nur unzureichend durch die extrahierten Faktoren erklärt werden, zudem stehen die eingestandenen bzw. entdeckten Malware-Probleme der Jahre 2004 und 2005 in einem engen Zusammenhang.

Die Verbindung zwischen dem fünften und siebten Faktor gibt ungefähr die Ergebnisse der ersten Analyse wieder, auch wenn sich hier eine andere Variable zur Variablengruppe des IT-Budget-Anteils gesellt und sich daraus eine neue Erkenntnis ergibt. Ein großzügiges Investitionsverhalten *(AntITS-11plus)* wird hier im siebten Faktor mit der Eigenschaft kombiniert, die PC-Anwender im Unternehmen über Gefahren aus dem Internet aufzuklären. Das hohe Investitionsvolumen kann also durchaus mit der Einstellung in Verbindung gebracht werden, durch die Aufklärung aller Mitarbeiter der Bedrohung aus dem Netz vorzubeugen.

Interessant hingegen ist die Veränderung, die sich aus dem achten Faktor ergibt, denn waren im ersten Durchgang die beiden Variablen noch schwach geladen mit drei anderen gemeinsam in einem Faktor abgebildet worden, weisen sie nun beide hohe Faktorladungen und annehmbare Kommunalitäten auf. Demnach scheinen Firmen, die selbst E-Commerce zur Aufgabe von Bestellungen bei anderen Unternehmen nutzen, einer höheren Spam-Belastung ausgesetzt zu sein. Tatsächlich ergibt eine bivariate Regression der beiden Variablen, dass Firmen, welche das Angebot des Online-Handels nutzen, einen signifikant um zehn Prozent höheren Spam-Anteil haben als Unternehmen, die auf diesen Service verzichten. In einer multivariaten Schätzung werden diese Ergebnisse in Abschnitt 5.3.3 bestätigt, dort erfolgt auch die Interpretation des Resultats. Besonders auffällig haben sich die Werte der Spam-Variablen verändert, so steigt die Kommunalität von 0,397 auf 0,589 und die hohe Faktorladung von 0,687 erlaubt eine eindeutige Zuordnung zu einem Faktor. Dagegen liegen die beiden höchsten Werte in Tabelle 5.10 betragsmäßig unter 0,34 und erklären damit zusammen weniger als 23 % der Varianz, also weniger als die Hälfte des einzelnen Faktors aus der zweiten Analyse. Hier unterscheiden sich demnach die Unternehmen, die in der Umfrage Zahlungs-

bereitschaften für IT-Sicherheit angegeben haben von jenen, die sich hierzu nicht geäußert haben.

Zu Beginn des Abschnitts wurde bereits erwähnt, dass die Kontrollvariable für den Sequencing-Effekt aufgrund ihrer zufälligen Verteilung auf die teilnehmenden Unternehmen eigentlich mit keiner in der Faktorenanalyse berücksichtigten Variablen in Zusammenhang stehen sollte. Anders ausgedrückt dürfte sie also nur mit einer hohen Faktorladung in einem Faktor auftauchen, der keine anderen Variablen miterklärt, und müsste gleichzeitig über eine hohe Kommunalität verfügen. Im Allgemeinen bleibt dabei die Frage offen, ob der Eigenwert des besagten Faktors knapp über oder unter eins liegt, da der Faktor bei einer Zufallsvariablen eigentlich eine exklusive Betrachtung einer einzigen Variablen vornimmt und somit theoretisch einen Eigenwert von genau eins besitzen müsste.

Im vorliegenden Fall liegt der Eigenwert für den elften (und letzten) extrahierten Faktor bei 1,009, und sowohl die Faktorladung von 0,885 als auch die Kommunalität von ungefähr 0,8 entsprechen den geforderten Erwartungen. Das Auftreten einer zwar betragsmäßig relativ geringen, aber dennoch nennenswerten Faktorladung von ca. 0,366 lässt jedoch aufhorchen, da der Faktor den Personalanteil der IT-Fachkräfte zu immerhin 13,4 % erklären kann.[7] Im Anschluss an die Betrachtung der Faktoren steht daher die zufällige Verteilung der Sequencing-Variablen und damit auch der Beobachtungsgruppen auf dem Prüfstand, da sich aus diesem Resultat ein zumindest schwacher Zusammenhang zwischen dieser und einer weiteren Variablen ableiten lässt. Darüber hinaus kann festgehalten werden, dass es sich bei diesem Wert um die höchste Faktorladung der Variablen unter den extrahierten Faktoren handelt.

Die übrigen Faktoren werden hier nicht weiter beschrieben, da ihre Zusammensetzung nur geringfügig von der vorigen Analyse abweicht. Zusammenfassend kann gesagt werden, dass die Faktorenanalyse nicht nur Variablen mit nachvollziehbarem Zusammenhang in Faktoren gemeinsam abgebildet, sondern potentielle Beziehungen aufgedeckt hat, welche im Vorfeld nicht zu erwarten waren. Diese möglichen Interdependenzen wurden anschließend in Regressionen untersucht, deren Resultate in Abschnitt 5.3 behandelt werden.

[7] Der anteilige Erklärungsgehalt einer Variablen durch einen Faktor ist gleich der quadrierten Faktorladung (siehe dazu auch Abschnitt 3.3.1).

5.2.3 Überprüfung der Sequencing-Variablen

Wie bereits auf den Seiten 62 bis 64 erläutert wurde, kann bei der Erhebung mehrerer Zahlungsbereitschaften bei CVM-Studien ein Sequencing-Effekt auftreten, welcher im Rahmen der vorliegenden Studie durch die Aufteilung von zwei auf vier Teil-Samples kontrolliert werden sollte. Inwiefern die Reihenfolge der Fragen einen signifikanten Einfluss auf die geäußerte *Willingness to pay* hatte, wird direkt im Anschluss an die hier angestellten Überlegungen betrachtet. Doch zunächst erfolgt eine genauere Untersuchung des Sachverhalts, dass sich in der Faktorenanalyse ein möglicher Zusammenhang zwischen der Sequencing-Variablen und dem Anteil der IT-Fachkräfte am gesamten Personal ergeben hat.

Die Indikatorvariable für den Sequencing-Effekt sollte eigentlich einer zufälligen Verteilung über die Unternehmen unterliegen und daher von anderen Variablen unabhängig sein, dem widersprechen jedoch zunächst die Erkenntnisse aus Tabelle 5.12. Doch die Auswertung der paarweisen Korrelationen dieser zentralen Variablen mit anderen Variablen genügt, um diese Zweifel umgehend wieder auszuräumen. In Tabelle 5.13 ist lediglich eine Auswahl all jener Variablen aufgelistet, deren Korrelationskoeffizienten zum Sequencing ein Signifikanzniveau von maximal zehn Prozent aufweisen.

	MalVorSpam	B2Cb	B2Cnein	AnzIT
B2Cb	0,1035**			
	(462)			
B2Cnein	-0,0938**	-0,8421***		
	(462)	(819)		
AnzIT	0,0982**	0,1002***	-0,0958***	
	(448)	(776)	(776)	
AntIT	0,0655	0,1057***	-0,1089***	0,1460***
	(435)	(739)	(739)	(751)

Erklärung: ***Signifikanz zum 1 %-Niveau, **Signifikanz zum 5 %-Niveau; Anz. Beob.in Klammern

Tabelle 5.13: Ausgewählte Korrelationen mit der Sequencing-Variablen

Abgesehen davon, dass nur Variablen aus zwei Themenbereichen signifikant mit der Sequencing-Variablen in Verbindung gebracht werden können, liegen ihre Korrelationskoeffizienten betragsmäßig bei maximal 0,11. Doch auch bei den in der Tabelle nicht berücksichtigten, da insignifikant mit dem Sequencing in Zusammenhang zu bringenden Variablen übersteigen die Betragswerte der Korrelationskoeffizienten den Wert von 0,11 nicht. Somit kann ob der niedrigen Korrelationswerte zumindest nicht mehr von einer linearen Abhängigkeit des Sequencing von anderen Einflussfaktoren ausgegangen werden. Die niedrigen Beobachtungszahlen bei den Korrelationen mit der Sequencing-Variablen sind durch das Antwortverhalten der Probanden bei den Zahlungsbereitschaften begründet, da anhand der erhobenen Ergebnisse nur für diese Unternehmen eine Zuordnung zu den Beobachtungsgruppen möglich (und sinnvoll) war.

Der Anteil der IT-Fachkräfte am Personalbestand der befragten Unternehmen, welcher in der Faktorenanalyse noch mit dem Sequencing in einem gemeinsamen Faktor abgebildet worden war, weist gemäß Tabelle 5.13 einen Korrelationskoeffizienten von weniger als 0,07 auf, dies ist der betragsmäßig kleinste unter den signifikanten Werten. Zwar verfügen die Zusammenhänge innerhalb der anderen hier wiedergegebenen Variablen größtenteils über eine höhere Signifikanz, doch mit Ausnahme des leicht nachvollziehbaren hohen Wertes von -0,84 beim E-Commerce liegen auch hier die Korrelationswerte mit betragsmäßig weniger als 0,15 relativ nahe bei null.

Aus den Resultaten dieser Überlegung ergibt sich, dass für die folgenden Untersuchungen davon ausgegangen werden kann, dass die Verteilung der Fragebögen nicht nur zufällig erfolgt war, sondern auch unterstellt werden kann, dass sich bei der Studie kein systematischer Fehler eingeschlichen hat. Insofern hat der aus der zweiten Faktorenanalyse entwickelte potentielle Zusammenhang zwischen dem Sequencing und dem Anteil des IT-Personals für den weiteren Verlauf der Untersuchungen keine tiefere Bedeutung, so dass das zu erwartende Auftreten des Sequencing-Effekts in der vorliegenden Studie weiterhin zu berücksichtigen ist. Der Analyse dieses für die Erhebung mehrerer Zahlungsbereitschaften typischen Phänomens widmet sich der nun folgende Abschnitt zur Regression.

5.3 Regressionsanalyse

Wird ein Unternehmen nach der Zahlungsbereitschaft für eine Dienstleistung gefragt, so kann davon ausgegangen werden, dass diese für Großunternehmen erheblich höher ausfällt als für kleine und mittlere Betriebe. Es steht somit außer Frage, dass die Unternehmensgröße eine entscheidende Rolle spielt, wie genau sie Einfluss auf das Antwortverhalten nimmt, soll im kommenden Abschnitt geklärt werden.

5.3.1 Untersuchung der Zahlungsbereitschaften

In der vom ZEW durchgeführten Umfrage wurden als Indikatoren für die Unternehmensgröße die Anzahl der Mitarbeiter und der Umsatz des Vorjahres abgefragt. Eigentlich könnte bei einer Korrelation von ca. 0,65 zwischen der Mitarbeiterzahl und dem Umsatz eines Unternehmens erwartet werden, dass die Regressionsergebnisse für die Zahlungsbereitschaft im Verhältnis zu diesen beiden Indikatoren der Unternehmensgröße eine gewisse Ähnlichkeit aufweisen. Wie aus den Tabellen 5.14 und 5.15 [8] klar hervorgeht, ist dies im vorliegenden Fall allerdings nicht gegeben, so dass hier zuerst und nur in Kürze auf die Zahlungsbereitschaft pro 1.000 Euro Umsatz eingegangen wird. Weitergehende Regressionen dieser relativen Zahlungsbereitschaften werden

	WTP pro 1.000 Euro Umsatz für Reduzierung von			
	Malware	**Std. Abw.**	**Spam**	**Std. Abw.**
um 30 %	4,39	8,47	2,45	4,35
um 50 %	13,23	8,18	6,73	4,32
um 70 %	10,56	7,23	3,77	3,82
um 90 %	19,61***	7,10	9,73***	3,79
Anz. Beob.	667		671	
(R^2) [8]	0,0187		0,0153	

Erklärung: ***Signifikanz zum 1 %-Niveau

Tabelle 5.14: Abgestufte Zahlungsbereitschaft pro 1.000 Euro Umsatz

[8] Es sei daran erinnert, dass im Folgenden die Bestimmtheitsmaße nur der Vollständigkeit halber angegeben werden, da eine sinnvolle Interpretation nicht möglich ist.

im weiteren Verlauf der Arbeit keine Berücksichtigung finden, da sie durchweg zu insignifikanten Ergebnissen geführt haben.

Gemäß Tabelle 5.14 sind die Schätzergebnisse für drei der vier prozentualen Angaben zur Reduzierung von Malware und Spam insignifikant, die Resultate für 30 % erreichen dabei in beiden Schätzungen sogar t-Werte von jeweils ungefähr 0,5. Wird nun eine weitere erklärende Variable in eines der beiden Regressionsmodelle aufgenommen, so wird hierdurch häufig auch das Ergebnis für die Verbesserung um 90 % insignifikant. Somit ergeben sich keine grundlegenden Unterschiede in der Zahlungsbereitschaft zwischen besonders umsatzstarken und umsatzschwachen Unternehmen. Die in den Tabellen 5.14 und 5.15 dargestellten Schätzungen stellen dabei nur eine erste Sondierung der zu wählenden Variablen dar, welche als Referenz für die Unternehmensgröße zu besseren, da aufgrund ihrer Signifikanz aussagekräftigeren Ergebnissen führen soll.

Ebenso wie in der ersten Schätzung wurden bei der Regression in Tabelle 5.15 nur die vier prozentualen Größen im Sondierungsmodell berücksichtigt, hier sind die Werte für die Zahlungsbereitschaft pro Mitarbeiter durchweg signifikant. Dabei scheitert lediglich der Wert für die Senkung des Spam-Aufkommens um 30 % mit einem P-Wert von 1,2 % nur knapp an der 1 %-Hürde, bei allen anderen Werten liegen die Fehlerwahrscheinlichkeiten unter 0,05 %. Daher wird im Folgenden die Konzentration auf diesen in Relation zur Unternehmensgröße gesetzten Zahlungsbereitschaften liegen.

	WTP pro Mitarbeiter für Reduzierung von			
	Malware	**Std. Abw.**	**Spam**	**Std. Abw.**
um 30 %	35,25***	10,06	19,32**	7,66
um 50 %	35,41***	9,87	27,89***	7,69
um 70 %	89,62***	8,62	53,21***	6,75
um 90 %	77,05***	8,54	58,40***	6,73
Anz. Beob.	742		742	
(R^2) [8]	0,2251		0,1754	

Erklärung: ***Signifikanz zum 1 %-Niveau, **Signifikanz zum 5 %-Niveau

Tabelle 5.15: Abgestufte Zahlungsbereitschaft pro Mitarbeiter

Werden nur diese ersten Resultate betrachtet, so fallen bereits ein paar Zusammenhänge ins Auge. Entgegen der Annahme der überproportionalen oder zumindest linearen Entwicklung der Werte liegen für die Bekämpfung der Malware-Gefahr die geäußerten Zahlungsbereitschaften für die beiden niedrigen Werte nahezu gleich, der Wert für 70 % übersteigt den für 90 % nicht unerheblich. Innerhalb der Beobachtungsgruppen jedoch bestätigt sich diese Annahme, so ist der Quotient für die beiden Versionen mit 30 und 70 % $\frac{89{,}62}{35{,}25} \approx 2{,}54 \geq 2{,}33 \approx \frac{7}{3}$, für die Versionen mit 50 und 90 % liegt er bei $\frac{77{,}05}{35{,}41} \approx 2{,}18 \geq 1{,}8 \approx \frac{9}{5}$.

Die kaum unterscheidbaren Schätzergebnisse für die beiden niedrigen Verbesserungspotentiale lassen vermuten, dass für einen schlechten, aus Sicht der Unternehmen vielleicht auch zu schlechten Schutz vor Malware, eine Zahlungsbereitschaft von immerhin 35 Euro besteht. Auf Basis dieser Werte dürften die jeweiligen Unternehmen dann ihre Entscheidung getroffen haben, welchen Mehrwert sie in der Verbesserung um das 1,3- bzw. das 0,8-fache sehen. Diese Vorgehensweise der Probanden würde erklären, warum die Schätzungen für eine Senkung der Malware-Bedrohung um 70 % so viel höher ausfallen als jene für 90 %.

Im Gegensatz zu den Ergebnissen für die Zahlungsbereitschaften für die Malware-Reduzierung steigen die geäußerten Werte für die Senkung des Spam-Anteils am E-Mail-Aufkommen streng monoton, die Quotienten betragen $\frac{53{,}21}{19{,}32} \approx 2{,}75 \geq 2{,}33 \approx \frac{7}{3}$ für 30 und 70 % respektive $\frac{58{,}40}{27{,}89} \approx 2{,}09 \geq 1{,}8 \approx \frac{9}{5}$ für 50 und 90 %. Aus den Antworten ergeben sich bei der Bekämpfung unerwünschter E-Mails Werte um 55 Euro für eine Verbesserung der Spam-Situation um 70 bzw. 90 %.

Wird dieses Resultat von ca. 55 Euro pro Mitarbeiter nun mit den in Abschnitt 2.2.1 diskutierten Ergebnissen von Clement et al. (2008) verglichen, so unterscheiden sich diese ungefähr um den Faktor neun. Diese enorme Diskrepanz kann jedoch durch die unterschiedlichen Lösungsansätze zur Eindämmung des Spam-Aufkommens durch Filtermaßnahmen erklärt werden. So unterstellt die im Rahmen der vorliegenden Studie formulierte Fragestellung eine (fiktive) zentralisierte Bekämpfung der Spam-Flut, während an der Kieler Universität tatsächlich dezentrale Maßnahmen gegen die unerwünschten E-Mails ergriffen worden sind. Somit ergibt sich aus dieser effizienteren

	WTP pro Mitarbeiter für Reduzierung von	
	Malware	**Std. Abw.**
um 70 %	55,35***	9,925
um 90 %	35,58***	10,47
AnzMalJahr	14,04***	4,352
AntITS0610	52,51***	13,52
B2CAnt	1,107***	0,312
MalVorSpam	19,72**	8,315
Anz. Beob.	657	
(R^2)	0,2687	

Erklärung: ***Signifikanz zum 1 %-Niveau, **Signifikanz zum 5 %-Niveau

Tabelle 5.16: Schrittweise Regression der WTP für Malware-Reduzierung

Vorgehensweise ein ungeheures Einsparungspotential an Arbeitszeit und somit an (Personal-)Kosten.

Nachdem diese Regressionen gezeigt haben, welche maßgebliche Rolle die Mitarbeiterzahl bei den geäußerten Zahlungsbereitschaften spielt, gilt es nun, weitere Einflussvariablen zu identifizieren. In schrittweise durchgeführten Regressionen wurden neben den Indikatoren für die unternehmensspezifische Bedrohungslage durch Malware und Spam weitere Variablen im Modell berücksichtigt, von denen eine Einflussnahme auf die geäußerten Zahlenwerte vermutet werden konnte. Dabei wurden die Zahlungsbereitschaften für eine Verbesserung um 30 und 50 % durchweg insignifikant, da bei gleichbleibenden Standardabweichungen die geschätzten Koeffizienten sanken.

Die Koeffizienten für die Reduzierung der Malware-Bedrohung um 30 bzw. 50 % wurden in Tabelle 5.16 nicht berücksichtigt, da die t-Werte jeweils unter 0,4 lagen. Nur geringen Veränderungen gegenüber der vorangegangenen Schätzung unterlagen hingegen die anderen beiden Prozentwerte, welche auf Basis der weggefallenen Koeffizienten nun als Differenz zu den niedrigen Zahlungsbereitschaften zu verstehen sind.

Die Tatsache, dass ein Unternehmen Vorfälle durch Schadprogramme zu vermelden hatte, steigert die Zahlungsbereitschaft der betroffenen Unternehmen erwartungsgemäß. Für jeden Beobachtungszeitraum, das heißt für die

beiden einzelnen Jahre 2005 und 2004 sowie für die Jahre vor 2004, in welchem die Unternehmen Probleme mit Malware hatten *(AnzMalJahr),* steigt ihre Zahlungsbereitschaft signifikant um 14 Euro pro Mitarbeiter. Somit sind Unternehmen, die in allen drei Zeiträumen mit Viren und Würmern zu kämpfen gehabt haben, dazu bereit, mit zusätzlichen 42 Euro je Mitarbeiter erheblich tiefer in die Tasche zu greifen als Betriebe ohne solche Vorfälle. Wurde dieser Zusammenhang mit den einzelnen Beobachtungszeiträumen getrennt voneinander untersucht, so lagen die genannten Geldsummen zwischen 19,98 Euro (vor 2004) und 26,31 Euro (2004), für das Jahr 2005 errechnete sich ein Betrag von 20,67 Euro. Aus der Tatsache, dass viele Unternehmen mehrfach Opfer von Schadprogrammen geworden waren, ergibt sich die Differenz des Mittelwertes dieser Einzelresultate zum obigen Ergebnis.

Die Gruppe der Unternehmen, welche angegeben haben, zwischen 6 und 10 % ihres IT-Budgets in IT-Sicherheit zu investieren *(AntITS0610),* ist mit einem Betrag von mehr als 50 Euro pro Angestelltem zu signifikant höheren Ausgaben bereit als die anderen Beobachtungsgruppen. Sie liegen damit auch über all jenen Betrieben, die mehr als 10 % ihrer IT-Ausgaben für Sicherheit aufbringen, wobei allerdings zu berücksichtigen ist, dass für die letztgenannten lediglich 100 Beobachtungen vorliegen gegenüber 214 mit einem relativ hohen Sicherheitsbewusstsein mit 6 bis 10 % Budget-Anteil.

Die Rolle des E-Commerce spielt bei der Zahlungsbereitschaft für die Eindämmung der Virengefahr ebenfalls eine große Rolle. Für jeden Prozentpunkt, welchen der Online-Handel am Umsatz eines Unternehmens ausmacht *(B2CAnt),* würde ein Unternehmen mehr als einen zusätzlichen Euro pro Mitarbeiter bezahlen. Von dieser zusätzlichen Investitionsbereitschaft wäre jedoch gemäß Abbildung B.9 in Anhang B nur jede vierte Firma betroffen, von denen wiederum nur bei 23 Betrieben der Jahresumsatz mindestens zur Hälfte durch E-Commerce erwirtschaftet wird. Die Abhängigkeit von dieser Form des Handels spiegelt sich hier also durch eine erhöhte Zahlungsbereitschaft für IT-Sicherheit wieder.

Zu guter Letzt hat die Reihenfolge der Fragestellung *(MalVorSpam)* einen signifikanten Einfluss auf die geäußerten Zahlungsbereitschaften, dies gilt ebenfalls für die Schätzung der *Willingness to pay* für die Reduzierung des Spam-Aufkommens in Tabelle 5.17. In beiden Fällen liegen die Koeffizienten

	WTP pro Mitarbeiter für Reduzierung von	
	Spam	**Std. Abw.**
um 30 %	12,81	9,631
um 50 %	18,42*	10,11
um 70 %	47,90***	9,109
um 90 %	47,72***	9,327
AntSpam	0,361***	0,148
AntSumAI	0,708***	0,263
AntITSkA	-22,10***	9,561
MalVorSpam	19,85**	7,518
Anz. Beob.	675	
(R^2)	0,2054	

Erklärung: ***Signifikanz zum 1 %-Niveau, **Signifikanz zum 5 %-Niveau, *Signifikanz zum 10 %-Niveau

Tabelle 5.17: Schrittweise Regression der WTP für Spam-Reduzierung

bei ungefähr +20 Euro, allerdings weist das gemeinsame positive Vorzeichen darauf hin, dass dieses Ergebnis in den beiden Regressionen unterschiedlich zu interpretieren ist. So tritt bei den Schadprogrammen die häufigere Art des Sequencing auf, bei welcher die zuerst geäußerte Zahlungsbereitschaft die höhere ist, die folgende aufgrund von Einkommenseffekten niedriger ausfällt.

Im Falle der unerwünschten E-Mails ist das Vorzeichen ebenfalls positiv, so dass die Antworten der Probanden um 20 Euro höher lagen, wenn zuerst nach der Zahlungsbereitschaft für die Reduzierung des Malware-Aufkommens gefragt wurde. Somit trifft die in den vorangegangenen Kapiteln beschriebene Vermutung, beim Thema Spam könnte durch die zuerst gestellte Frage nach Malware eine Art von Sensibilisierung stattfinden, hier tatsächlich zu, die umgekehrte Form des Sequencing liegt vor.

Auch bei der Regression zur Reduzierung von Spam sind die Koeffizienten für 30 und 50 % nicht mehr oder nur schwach signifikant, dennoch finden sie sich in Tabelle 5.17. Insofern sind die Angaben für 70 und 90 % auch nicht in Relation zu den anderen Werten zu verstehen, sondern können absolut interpretiert werden, die Zahlungsbereitschaften für die jeweils höheren erfragten Verbesserungspotentiale liegen damit bei knapp 48 Euro.

Analog zum Auftreten von Malware-Befall ist auch bei unerwünschten E-Mails eindeutig ein Ursache-Wirkung-Prinzip zu erkennen. So steigt mit zunehmendem Spam-Anteil *(AntSpam)* am täglichen E-Mail-Aufkommen die Zahlungsbereitschaft für die Bekämpfung desselben proportional, jeder zusätzliche Prozentpunkt an Spam erhöht die *Willingness to pay* um 36 (Euro-) Cent. Dies entspricht bei einem Median von 15 % Werbe-Mails einem Betrag von 5,41 Euro, für Unternehmen mit mehr unerwünschten als erwünschten E-Mails steigt die Zahlungsbereitschaft somit um 18 bis 36 Euro für jeden seiner Mitarbeiter.

Ebenfalls einen hochsignifikanten Einfluss hat der Anteil der Administrationskräfte, die in einem Betrieb beschäftigt werden, unabhängig davon, ob sie für allgemeine Aufgaben in der IT-Betreuung, für IT-Sicherheit oder für beide Bereiche verantwortlich sind *(AntSumAI).* Dieser Einfluss wirkt sich jedoch nur geringfügig aus, so vergrößert sich zwar mit steigendem Anteil der Administratoren die Zahlungsbereitschaft, bedingt durch den Median von 2,9 % erhöht sich die Zahlungsbereitschaft bei jedem zweiten Unternehmen dadurch aber nur um bis zu zwei Euro pro Mitarbeiter. Daraus lässt sich jedoch schließen, dass unter der in der Fragestellung getroffenen Annahme, dass ein eigener Schutz nicht möglich sei, die Firmen ihre Investitionen in IT-Sicherheit von den eigenen Administratoren in die fiktive europäische Institution umschichten würden. Je mehr Mittel demnach bislang in eigene Maßnahmen zur Bekämpfung der Spam-Flut geflossen waren, desto mehr sollte auch weiterhin dem Schutz vor unerwünschten E-Mails zugutekommen. Möglichweise wird auch der zeitliche Aufwand der Pflege von Filtermaßnahmen nach ihrer Installation und Konfiguration als verhältnismäßig gering eingeschätzt.

Als letzte erklärende Variable für die Zahlungsbereitschaft zur Reduzierung der Spam-Mails sei noch das Investitionsverhalten in IT-Sicherheit genannt. Während es beim Kampf gegen Schadprogramme die Unternehmen mit sechs bis zehn Prozent Anteil der IT-Sicherheit am IT-Budget waren, die signifikant in das Regressionsmodell einflossen, stechen hier jene Unternehmen hervor, die zu ihren Investitionen in IT-Sicherheit keine Angaben machen konnten oder wollten *(AntITSkA).* Die *Willingness to pay* dieser Firmen lag im Vergleich zu den anderen Betrieben um 22 Euro pro Person niedriger.

WTP Malware	**30 %**	**50 %**	**70 %**	**90 %**
AnzMA	23,21***	49,09***	66,84***	90,85***
	(4,133)	(3,777)	(6,409)	(6,254)
$AnzMA^2$	-0,0014***	-0,0060***	-0,0032***	-0,0103***
	(0,0003)	(0,0005)	(0,0005)	(0,0008)
Anz. Beob.	148	155	204	208
(R^2)	0,4266	0,5250	0,8370	0,5360

Erklärung: ***Signifikanz zum 1 %-Niveau, Std. Abw. in Klammern

Tabelle 5.18: Einzelne Zahlungsbereitschaften für Malware-Reduzierung

Aus diesem negativen Wert könnte nun geschlossen werden, dass bei diesen Unternehmen eine geringere Bereitschaft vorliegt, finanzielle Mittel für die IT-Sicherheit des Unternehmens freizugeben. Andererseits ist jedoch auch denkbar, dass die Personen, welche in den Fragebögen keine Angaben zum Investitionsanteil gemacht haben, tatsächlich keinen Einblick in die Budgetierung der IT-Abteilung haben. Aus diesem Grund könnten diese Probanden die Kosten, die durch IT-Sicherheit verursacht werden, niedriger eingestuft haben als jene, die einen Einblick in die Kostenstruktur des IT-Bereichs und in die dort getätigten Investitionen haben.

In Abschnitt 2.3 wurde bereits die Möglichkeit angesprochen, dass bei größeren Unternehmen Skaleneffekte Einfluss auf die geäußerten Zahlungsbereitschaften nehmen könnten. Dieser Gedanke soll nun in den folgenden beiden Schätzungen aufgegriffen werden, welche in den Tabellen 5.18 sowie 5.19 wiedergegeben sind. Hierfür wurde für jeden der erfragten Prozentwerte die Zahlungsbereitschaft auf die Anzahl der Mitarbeiter *(AnzMA)* sowie deren Quadrat *($AnzMA^2$)* regressiert, um zu überprüfen, ob mit wachsendem Personalbestand die angegebenen Geldsummen kleiner werden.

Erwartungsgemäß ist die Anzahl der Mitarbeiter in beiden Tabellen durchweg hochsignifikant, für die Quadrate der Mitarbeiterzahl trifft das ebenfalls zu. Durch die negativen Vorzeichen vor den betragsmäßig kleinen Koeffizienten der quadrierten Werte lässt sich der Skaleneffekt nachweisen, den die befragten Unternehmen mit zunehmender Größe als Einsparungspotential zu identifizieren scheinen. Entgegen der Resultate der vorangegangenen

WTP Spam	**30 %**	**50 %**	**70 %**	**90 %**
AnzMA	12,41***	23,31***	28,70***	48,98***
	(2,157)	(1,891)	(4,360)	(3,290)
$AnzMA^2$	-0,0008***	-0,0028***	-0,0019***	-0,0057***
	(0,0002)	(0,0002)	(0,0003)	(0,0004)
Anz. Beob.	142	151	189	199
(R^2)	0,2422	0,5053	0,2192	0,5521

Erklärung: ***Signifikanz zum 1 %-Niveau, Std. Abw. in Klammern

Tabelle 5.19: Einzelne Zahlungsbereitschaften für Spam-Reduzierung

Regression für die Bekämpfung von Schadprogrammen zeichnet sich für beide Zahlungsbereitschaften eine strenge Monotonie der Schätzwerte für die Mitarbeiterzahl ab, dagegen entwickeln sich die Werte der quadrierten Mitarbeiterzahl nicht monoton.

Obwohl sich für alle acht einzelnen Regressionen signifikante Koeffizienten für die quadrierte Mitarbeiterzahl ergeben, stellt sich die Frage, inwiefern dieser Einfluss maßgeblichen Charakter hat. Als Beispiel werden die Funktionswerte für 90 % Reduzierung von Malware und Spam herangezogen, für welche die Resultate sowohl für die Mitarbeiterzahl als auch für ihr Quadrat absolut gesehen am höchsten sind, um ihren maximalen Einfluss auf die gesamte Zahlungsbereitschaft eines Unternehmens für all seine Mitarbeiter hochzurechnen. Für den Median von 20 Mitarbeitern ergibt sich ein Einsparungspotential von 4,13 Euro für Malware sowie 2,27 Euro für Spam bei 1.817 Euro bzw. 980 Euro Zahlungsbereitschaft für den nicht-quadrierten Wert. Für die Hälfte der befragten Unternehmen bedeutet dies einen Anteil von 0,2 % an der gesamten Zahlungsbereitschaft, bei einer Unternehmensgröße von 100 Mitarbeitern, die nur von dreizehn Prozent der Firmen erreicht wird, liegt der Anteil bei 1,1 %.

Entsprechend der Verteilung der Unternehmensgrößen liegt damit für 95 % der Unternehmen der durch eventuelle Skaleneffekte eingesparte Anteil der Zahlungsbereitschaft unter 2,7 %. Insofern können zwar in der vorliegenden Studie Unternehmen mit wachsendem Personalbestand ihre Kosten für IT-Sicherheit senken, diese Einsparungen fallen jedoch kaum ins Gewicht. Auf Basis der Resultate der Tabellen 5.18 und 5.19 könnte nun der Versuch

unternommen werden, analog zu den in Abschnitt 3.2.4 vorgestellten Studien die Kosten einer einhundertprozentigen Behebung des Problems zu schätzen. Demnach dürften die Ergebnisse bei ungefähr 100 Euro für den theoretischen vollständigen Schutz vor Malware liegen, gegenüber etwa 50 Euro für das erfolgreiche Ausfiltern aller Spam-Mails, diese konservative Schätzung kann dabei als untere Schranke der Kosten angesehen werden.

Dabei gilt es zu beachten, dass die Einrichtung eines so effizienten Spam-Filters – insbesondere in Verbindung mit dem verantwortungsvollen Umgang mit E-Mail-Adressen – durchaus im Bereich des Möglichen liegt, ein so zuverlässiger Schutz vor Schadprogrammen jedoch kaum zu realisieren sein dürfte. Zwar hat sich die Qualität der Virenschutzprogramme in den vergangenen drei Jahrzehnten kontinuierlich verbessert, trotzdem können diese bei besonders innovativen Veränderungen der Malware zumindest vorübergehend mit ernstzunehmenden Problemen konfrontiert werden. Dennoch sollten diese Ergebnisse Beachtung finden, da eine vollständige Vermeidung sämtlicher Tötungsdelikte, wie sie in anderen CVM-Studien angenommen wurde, gleichermaßen unrealistisch und vielmehr eine theoretische Zielsetzung ist.

5.3.2 Beleuchtung der Vorfälle durch Malware

In diesem Abschnitt wird untersucht, welche der erhobenen Variablen mit den Vorfällen durch Schadprogramme in den Jahren 2005 und 2004 sowie vor 2004 zusammenhängen und wodurch sich erklären lässt, dass die Hälfte der befragten Unternehmen angegeben hat, noch nie Vorfälle mit Schadprogrammen gehabt zu haben. Dazu wurden im ersten Durchgang jeweils Modelle mit allen Variablen entwickelt, die möglicherweise einen Einfluss auf die Wahrscheinlichkeit haben, von Schadprogrammen betroffen gewesen oder verschont geblieben zu sein. In einer schrittweisen Regression zum Signifikanzniveau von 10 % sollten sich dann die relevanten Einflussfaktoren herauskristallisieren, welche in den Tabellen dieses Abschnitts wiedergegeben sind. Während zunächst auch Vorfälle durch Schadprogramme im direkt vorangegangenen Beobachtungszeitraum als erklärende Variable ins Schätzmodell einflossen, wurde diese Indikatorvariable im zweiten Schritt aus dem Modell ausgeschlossen, damit die Ergebnisse nicht zu sehr von diesem starken Einfluss geprägt werden.

Malware 2005	**schrittw.**	**Std. Abw.**	**schrittw.**	**Std. Abw.**
Mal2004 (b)	0,4706***	0,0370	[ohne Mal2004]	
MalVor2004 (b)			0,1558***	0,0387
B:EDV (b)	-0,1184***	0,0461	-0,1661***	0,0441
AntITSkA (b)			-0,0898***	0,0347
B2CAnt			0,0019*	0,0011
Anz. Beob.	807		724	
Pseudo-R^2	0,1827		0,0451	
Log Likelihood	-379,8		-399,9	

Erklärung: ***Signifikanz zum 1 %-Niveau, *Signifikanz zum 10 %-Niveau, (b) binäre Variable

Tabelle 5.20: Logit-Schätzung zu Malware-Vorfällen im Jahr 2005

Aus der in Tabelle 5.20 dargestellten ersten Regression gehen zunächst zwei signifikante Einflussfaktoren für Malware-Probleme im Jahr 2005 hervor, bei denen sich bereits die eben beschriebene Vermutung bestätigt. Demnach hatten Unternehmen, die bereits im Vorjahr Vorfälle durch Schadprogramme gehabt hatten *(Mal2004),* im Jahr 2005 eine um 47 % höhere Wahrscheinlichkeit, wieder von Viren, Würmern oder Trojanern betroffen zu sein. Zusätzlich hob sich bei dieser Schätzung mit den Bereichen „Software und IT-Dienste“ ein Wirtschaftszweig von den anderen Dienstleistern ab. Je nach Modell hatten die Unternehmen aus der EDV-Branche *(B:EDV)* eine um 12 bis 17 % geringere Wahrscheinlichkeit eines Malware-Befalls, was aufgrund der Tatsache, in gleichem Maße den Bedrohungen aus dem Internet ausgesetzt zu sein, auf einen besseren bzw. effektiveren Schutz zurückgeführt werden kann. Das Pseudo-Bestimmtheitsmaß von 0,18 bescheinigt der Schätzung eine akzeptable Aussagekraft für ein so schwer vorhersagbares Ereignis wie den Befall eines (geschützten) Computers durch Malware. Vor Allem in Hinblick auf die Bestimmtheitsmaße der weiteren Ergebnisse dieses Abschnitts unterstreicht die Schätzung damit noch einmal den engen Zusammenhang zwischen Vorfällen in den Jahren 2004 und 2005.

Der hochsignifikante Zusammenhang zwischen Malware-Vorfällen in benachbarten Beobachtungszeiträumen zieht sich dabei wie ein roter Faden durch die Regressionen der verschiedenen Jahre. Demnach sind Probleme mit Schadprogrammen kein kurzfristiges Phänomen, das schnell aus der Welt

geschafft werden kann, sondern vielmehr die Umsetzung umfangreicher Maßnahmen verlangt. Insofern können wiederholte Vorfälle durch Malware darauf zurückgeführt werden, dass ein unzureichender Schutz längerfristig nicht als solcher erkannt worden ist.

In der zweiten Regression, in welcher die Vorfälle im Jahr 2004 bewusst ausgeklammert wurden, ergibt sich aus dem Fehlen dieses Zeitraums ein signifikanter Zusammenhang mit den Jahren vor 2004 *(MalVor2004)*. Darüber hinaus hat die Tatsache, dass ein Unternehmen eine Aussage über den Anteil der IT-Sicherheit an seinem IT-Budget verweigert hat *(AntITSkA)*,[9] einen signifikanten Einfluss auf eben diese Malware-Wahrscheinlichkeit. Überraschend ist in diesem Zusammenhang, dass jene Firmen eine um neun Prozent geringere Wahrscheinlichkeit hatten, im Jahr 2005 Probleme mit Schadprogrammen gehabt zu haben. Dieses Phänomen wiederholt sich bei den weiteren Schätzungen mit Werten zwischen sechs und zwölf Prozent unter Wahrung des Vorzeichens. Somit wurden bei Betrieben, die über ihre Investitionen in IT-Sicherheit keine Auskunft geben wollten oder konnten, über die Jahre hinweg signifikant weniger Vorfälle durch Malware registriert als bei den anderen Probanden der Studie.

Eine mögliche Begründung für diesen weniger offensichtlichen Zusammenhang könnte sein, dass diese Unternehmen entweder mit keinem festen IT-Budget planen oder innerhalb dieses Budgets keinen fixen Anteil für IT-Sicherheit festgelegt haben. Diese Annahme würde für flexibel planende Betriebe zutreffen, die ihre Ausgaben für Informationstechnologie bzw. deren Absicherung nicht anhand von starren Regeln bestimmen, sondern die Mittel je nach Bedarf zur Verfügung stellen. Für die umgekehrte Richtung der Kausalität gibt es hingegen keine plausible Erklärung – warum sollte ein Unternehmen, wenn es keine Malware-Vorfälle zu beklagen hat, keine Auskunft über seinen Budget-Anteil für IT-Sicherheit erteilen.

Zuletzt gibt es noch einen nur schwach signifikanten Zusammenhang zwischen Malware-Vorfällen und dem Umsatzanteil des E-Commerce *(B2CAnt)*. Demnach stieg mit wachsender Abhängigkeit vom Online-Handel, beispielsweise durch die leichtere Erreichbarkeit der eigenen IT-Infrastruktur von

[9] Es handelt sich dabei ausschließlich um Unternehmen, welche im Fragebogen die Antwortmöglichkeit „keine Angabe“ angekreuzt haben, *nicht* um Missings.

Malware 2004	**schrittw.**	**Std. Abw.**	**schrittw.**	**Std. Abw.**
MalVor2004 (b)	0,2614***	0,0387	[ohne MalVor2004]	
B2Cnein (b)	-0,0677**	0,0338	-0,0656**	0,0335
AntITSkA (b)	-0,0592*	0,0356	-0,0855**	0,0343
B:EDV (b)	-0,1019**	0,0496	-0,1065**	0,0502
Anz. Beob.	744		744	
Pseudo-R^2	0,0746		0,0166	
Log Likelihood	-397,0		-421,9	

Erklärung: ***Signifikanz zum 1 %-Niveau, **Signif. zum 5 %-Niveau, *Signif. zum 10 %-Niveau, (b) binäre Variable

Tabelle 5.21: Logit-Schätzung zu Malware-Vorfällen im Jahr 2004

außen, auch das Risiko, Opfer von Malware-Befall zu werden.

Die größere Wahrscheinlichkeit, mit durch Schadprogramme verursachten Problemen konfrontiert zu sein, wenn es bereits im Vorjahr Vorfälle gegeben hatte, lag entsprechend Tabelle 5.21 auch im Jahr 2004 vor. Demnach hatten Unternehmen, bei denen es bereits vor 2004 zu Problemen durch Malware gekommen war, für das Jahr 2004 eine um 26 % höhere Wahrscheinlichkeit, wieder Opfer von Viren, Würmern oder Trojanern zu werden.

Wie schon im Jahr 2005 fallen neben den Unternehmen, welche keine Angaben zu ihrem Budget für IT-Sicherheit gemacht haben, auch hier die Mitglieder der EDV-Branche wieder positiv auf. Ähnlich wie in der vorangegangenen Regression hatten sie gegenüber den anderen Wirtschaftszweigen eine um zehn bis elf Prozent größere Chance, im Jahr 2004 nicht von Schadprogrammen betroffen gewesen zu sein, was die bereits geäußerte Vermutung stützt, dass sich diese Unternehmen besser gegen Malware schützen bzw. geschützt haben.

Die schwach signifikante Abhängigkeit der Wahrscheinlichkeit von Malware-Vorfällen im Jahr 2005 vom Umsatz-Anteil durch E-Commerce wird im Jahr 2004 durch die Absenz vom Online-Handel *(B2Cnein)* substituiert. Somit sank 2004 die Malware-Gefahr für Unternehmen, die sich gegen das Anbieten einer E-Commerce-Plattform entschieden haben, um fast sieben Prozent, dementsprechend ist auch das Auftreten des Vorzeichenwechsels offensichtlich nachvollziehbar.

Malware vor 2004	**schrittw.**	**Std. Abw.**	**kausal**	**Std. Abw.**
ITBerat (b)	*0,0766***	*0,0346*		
WBAdmin (b)	*0,0938****	*0,0344*		
AntITSkA (b)	-0,1140***	0,0359	-0,1189***	0,0341
Anz. Beob.	720		756	
Pseudo-R^2	0,0245		0,0121	
Log Likelihood	-424,8		-445,9	

Erklärung: ***Signifikanz zum 1 %-Niveau, **Signifikanz zum 5 %-Niveau, (b) binäre Variable

Tabelle 5.22: Logit-Schätzung zu Malware-Vorfällen vor 2004

Bei den Schätzungen zu Vorfällen durch Malware im Zeitraum vor 2004, deren Resultate in Tabelle 5.22 wiedergegeben sind, ergaben sich Zusammenhänge, deren Kausalitäten je nach Vorzeichen unterschiedlich zu interpretieren sind. So wurde in den schrittweise generierten Regressionsmodellen die Variable zur IT-Beratung *(ITBerat)* berücksichtigt, um überprüfen zu können, ob Unternehmen, die sich in Fragen der IT-Sicherheit von externer Seite beraten lassen, dadurch eine geringere Wahrscheinlichkeit haben, Opfer von Schadprogrammen zu werden. Zwar ergab sich im abgebildeten Schätzmodell ein signifikanter Zusammenhang, das Ergebnis müsste in dieser Form jedoch dergestalt interpretiert werden, als dass Unternehmen, die sich Beratung im Bereich IT-Sicherheit einholen, *dann* eine höhere Wahrscheinlichkeit für Malware-Vorfälle haben. In der umgekehrten Richtung hingegen klingt die Schlussfolgerung plausibel, das heißt, dass Betriebe, *nachdem* sie Probleme mit Schadprogrammen gehabt hatten, die Hilfe von IT-Experten in Anspruch genommen haben. Ein solcher Zusammenhang konnte im Vorfeld der Regression lediglich vermutet werden, da sich aus der deskriptiven Betrachtung der Zusammenhänge ein Korrelationskoeffizient von +0,05 ergeben hatte, welcher jedoch insignifikant war.

Ähnlich verhält es sich für die Weiterbildung der Administratoren *(WB-Admin),* die ebenfalls nur sehr schwach positiv mit den Malware-Vorfällen vor 2004 korreliert war. Der positive Zusammenhang mit Vorfällen durch Malware in früheren Jahren kann nur dann sinnvoll interpretiert werden, wenn angenommen wird, dass Unternehmen als Reaktion auf die Probleme ihrem IT-Personal eine Fortbildung ermöglichen.

Aus diesem Grund mussten die beiden genannten sowie weitere Variablen, die aufgrund ihrer Insignifikanz hier nicht berücksichtigt worden sind, aus dem Regressionsmodell entfernt werden. Die Ergebnisse der Regression, bei welcher für alle Variablen die richtige Richtung der Kausalität gewährleistet ist, sind in der rechten Spalte der Tabelle wiedergegeben. Hier verbleibt als einzige erklärende Variable die bereits in den anderen Schätzungen zur Auftrittswahrscheinlichkeit von Malware aufgetretene Eigenschaft, über den Anteil am IT-Budget, der in IT-Sicherheit investiert wird, keine Angaben gemacht zu haben. Weitere signifikante Variablen, die einen Einfluss auf die Wahrscheinlichkeit von Sicherheitsproblemen in den Jahren bis 2003 gehabt haben, konnten hier nicht gefunden werden. Da jedoch die Angaben in den Fragebögen eine Zustandsbeschreibung zum Zeitpunkt der Erhebung waren, dieser Zustand aber zwei Jahre zuvor nicht zwangsläufig der gleiche gewesen sein muss, können einige der Variablen die gegenwärtige Situation besser erklären als die Vergangenheit. Auch führen Entscheidungen wie das Nutzen von IT-Beratung oft nicht sofort zu Veränderungen, wenn beispielsweise im Zusammenhang mit der Beratung umgesetzte Maßnahmen erst greifen müssen.

Bei den Unternehmen, die nach eigenen Angaben noch nie Vorfälle durch Schadprogramme zu beklagen hatten, gehen die EDV-Unternehmen als die Variable mit dem größten Koeffizienten hervor, wie aus Tabelle 5.23 entnommen werden kann. Demnach haben die Mitglieder der EDV-Branche mit fast 18 % ein erheblich geringeres Risiko, von Malware betroffen zu sein, als die Firmen der anderen Wirtschaftszweige.

Doch auch beim Versuch, die Voraussetzungen dafür zu identifizieren, bislang von Malware verschont geblieben zu sein, sind in der ersten schrittweisen Regression mehrere Variablen im Modell enthalten, die in Anbetracht der Vorzeichen der Ergebnisse nicht erklärend wirken. So ergibt es keinen Sinn, dass Unternehmen, die IT-Beratung nutzen, ihre Administratoren weiterbilden lassen oder ihre Anwender über Gefahren aus dem Internet aufklären *(AufkAnw),* eine geringere Wahrscheinlichkeit haben, noch keine Vorfälle durch Schadprogramme gehabt zu haben. In dieser Konstellation wäre also die Fortbildung und Aufklärung von Mitarbeitern über Gefahren als ursächlich für Probleme mit Viren, Würmern oder Trojanern zu erachten.

keine Malware	**schrittw.**	**Std. Abw.**	**kausal**	**Std. Abw.**
B2B (b)	-0,0765*	0,0450	-0,1150***	0,0410
B2Cnein (b)	0,0801*	0,0414		
ITBerat (b)	*-0,1102***	*0,0400*		
WBAdmin (b)	*-0,0822***	*0,0387*		
AufkAnw (b)	*-0,0740**	*0,0396*		
B:EDV (b)	0,1737**	0,0689	0,1790***	0,0652
AntITSkA (b)			0,0776*	0,0418
Anz. Beob.	718		734	
Pseudo-R^2	0,0337		0,0196	
Log Likelihood	-480,6		-498,4	

Erklärung: ***Signifikanz zum 1 %-Niveau, **Signif. zum 5 %-Niveau, *Signif. zum 10 %-Niveau, (b) binäre Variable

Tabelle 5.23: Logit-Schätzung für keine Malware-Vorfälle

Vielmehr beschreibt dieser Zusammenhang die Verbesserung der Sicherheitsmaßnahmen wie Beratung und Weiterbildung als reaktives Verhalten nach Problemen mit Malware. Somit hat also beispielsweise nicht in umgekehrter Richtung eine Aufklärung der Mitarbeiter als präventive Maßnahme *vor* einem ersten Zwischenfall die Chancen verbessert, zukünftig von Schadprogrammen verschont zu bleiben.

Wie schon im vorangegangenen ersten Regressionsansatz lag ein solcher Zusammenhang im Bereich des Möglichen, da die entsprechenden Korrelationskoeffizienten bei betragsmäßigen sehr kleinen Werten von maximal 0,1 durchweg mit einem negativen Vorzeichen versehen waren. Doch erst die hier durchgeführte Regression konnte endgültige Sicherheit geben, dass sich im multivariaten Modell nicht doch ein positiver Zusammenhang in Verbindung mit weiteren Regressoren durch deren Zusammenspiel entwickelt.

Nachdem aus dem Regressionsmodell alle potentiell Einfluss nehmenden Variablen entfernt wurden, für welche die Kausalität nicht wie gewünscht gegeben ist, konnte neben zwei bislang wiederholt in Erscheinung getretenen Indikatoren eine neue relevante Eigenschaft identifiziert werden. So liegt die Wahrscheinlichkeit, noch nie Probleme mit Schadprogrammen gehabt zu haben, bei Unternehmen um 11,5 % niedriger, wenn sie das E-Commerce-

Angebot anderer Firmen nutzen. Das heißt umgekehrt, dass bei Firmen, welche auf die Nutzung dieses Angebots verzichten und somit vielleicht im Umgang mit dem Internet vorsichtiger oder in Fragen der Sicherheit restriktiver sind, die Chancen entsprechend größer sind, bis dato noch keine durch Viren, Würmer oder Trojaner verschuldete Vorfälle gehabt zu haben. Hier wirkt sich demnach die Nichtteilnahme am E-Commerce und der möglicherweise aufmerksamere Umgang mit dem Internet als Präventionsmaßnahme gegen Malware aus.

Nach Betrachtung dieser vier Regressionen kann festgestellt werden, dass sich für die Größe des Personalbestands kein signifikanter Zusammenhang mit der Wahrscheinlichkeit ergeben hat, Probleme mit Schadprogrammen gehabt zu haben. So bieten kleine Betriebe mit wenigen Rechnern einerseits weniger Angriffsfläche, verfügen oft aber auch nicht über ausreichend geschultes Personal im Bereich der IT-Sicherheit. Große Unternehmen mit entsprechend mehr Benutzern und Computern und somit mehr potentiellen Schwachstellen in der Kette der IT-Sicherheit können demnach mit koordinierten Sicherheitsmaßnahmen in eigenen IT-(Sicherheits-)Abteilungen die Wahrscheinlichkeit des Malware-Befalls auf das gleiche Niveau senken.

Zusammenfassend kann für die Jahre 2004 und 2005 festgestellt werden, dass sich – sowohl die Koeffizienten betreffend als auch in Bezug auf die Signifikanzniveaus – in jeder Regression ein vorangegangener Beobachtungszeitraum als die wichtigste erklärende Variable herausgestellt hat. Vorfälle durch Schadprogramme sind somit also kein Produkt des Zufalls, sondern treffen immer wieder die gleichen Opfer. Diese Unternehmen sollten daher unbedingt ihre Sicherheitsrichtlinien und Vorkehrungen zum Schutz ihrer IT-Infrastruktur überdenken und vielleicht auch vermehrt die Unterstützung von IT-Experten suchen. Die Resultate für die IT-Beratung in den Tabellen 5.22 und 5.23 sind ein Hinweis dafür, dass diese Maßnahme bereits in einigen Unternehmen umgesetzt wurde. Ähnlich verhält es sich für die Weiterbildung der Administratoren, da auch hier festgestellt werden konnte, dass nicht die Weiterbildung als erfolgreiche Präventionsmaßnahme identifiziert werden konnte, sondern vielmehr die Unternehmen, die bereits Erfahrungen mit Schadprogrammen machen mussten, ihr Personal schulen, um weitere Vorfälle zu vermeiden.

5.3.3 Betrachtung des Spam-Anteils

Bei der Faktorenanalyse in Abschnitt 5.2 wurde bereits festgestellt, dass ein Zusammenhang zwischen der Nutzung der Online-Angebote anderer und dem Spam-Anteil am E-Mail-Aufkommen bestehen könnte. Das Ergebnis der Regression in Tabelle 5.24 bestätigt diese Vermutung, da der Anteil der Spam-Mails bei Unternehmen, welche selbst Bestellungen im Internet aufgeben *(B2B),* um knapp zehn Prozent höher liegt als bei den Unternehmen, die auf das E-Commerce-Angebot anderer verzichten. Dieser Zusammenhang könnte damit erklärt werden, dass Personen, die im Internet Bestellungen aufgeben, meist bereitwillig ihre E-Mail-Adresse weitergeben und somit für deren Verbreitung sorgen. Ob es sich dann beispielsweise um die (teilweise unrechtmäßige) Weitergabe von erhaltenen Adressen durch die Anbieter oder den sorglosen Umgang der Anwender mit persönlichen Daten handelt, sei in diesem Fall dahingestellt.

Durch die im Vorfeld der Regressionen durchgeführten Faktorenanalysen war es – im Gegensatz zu den Untersuchungen zu Vorfällen durch Schadprogramme – möglich, anhand der extrahierten Faktoren bestimmte Variablen aus der Liste potentieller Regressoren zu entfernen. So wäre beispielsweise denkbar gewesen, dass Unternehmen mit einem höheren Anteil an IT-Fachkräften durch deren Bewusstsein für die verschiedenen Bedrohungen aus dem Internet und infolgedessen einem umsichtigeren Umgang mit der eigenen E-Mail-Adresse ein geringeres Spam-Volumen zu bewältigen hätten. Doch der positive Zusammenhang aus der Faktorenanalyse in Tabelle 5.10 ließ bereits Gegenteiliges vermuten, und in einer bivariaten Regression bestätigte sich diese lineare Abhängigkeit mit einem signifikanten positiven Wert. Ähnliches gilt für den Anteil der Administratoren am Personal, so dass in beiden Fällen lediglich die umgekehrte Kausalität unterstellt werden kann, also dass ein größeres Spam-Aufkommen die Einstellung von IT-Experten auf den Plan ruft. Im Gegensatz dazu erscheint die Abhängigkeit des Spam-Anteils von der IT-Beratung *(ITBerat)* mit umgekehrtem Vorzeichen auch in ihrer Kausalität plausibel, da sich aus dieser Beziehung ableiten ließe, dass der Anteil der unerwünschten E-Mails am gesamten Mail-Aufkommen bei beratenen Unternehmen geringer ausfallen sollte.

Spam-Anteil	**schrittw.**	**Std. Abw.**
MalVor2004 (b)	5,624***	2,099
B2CAnt	0,158**	0,063
B2B (b)	9,856***	2,179
ITBerat (b)	-5,872***	2,010
Konstante	20,02***	2,329
Anz. Beob.	655	
Korr. R^2	0,0640	

Erklärung: ***Signifikanz zum 1 %-Niveau, **Signifikanz zum 5 %-Niveau, (b) binäre Variable

Tabelle 5.24: Schrittweise OLS-Schätzung des Spam-Anteils

Wie bereits erwähnt hat im endgültigen schrittweise entwickelten Regressionsmodell das Nutzen von E-Commerce einen signifikanten Einfluss auf die Spam-Quote, der abgesehen von der Konstanten sowohl den höchsten Koeffizienten als auch die höchste Signifikanz besitzt. Doch auch das Anbieten der Möglichkeit des elektronischen Handels wirkt sich nachteilig auf den eigenen Spam-Anteil aus, wenn auch der tatsächliche Effekt ein vernachlässigbar geringes Ausmaß annimmt. So steigt mit jedem Prozentpunkt, welchen der Online-Handel am Gesamtumsatz *(B2CAnt)* ausmacht, der Anteil der unerwünschten E-Mails am täglichen Mail-Aufkommen um 0,13 % und betrifft gemäß Abbildung B.9 lediglich ein Viertel der teilnehmenden Unternehmen. Demnach hat insgesamt nur jedes 30. Unternehmen einen Anstieg des Spam-Volumens von mehr als fünf Prozent hinzunehmen.

Dagegen können Unternehmen, die sich von Experten zu Fragen der IT-Sicherheit beraten lassen, den Anteil der Spam-Mails, welche sie täglich erhalten, um fast sechs Prozent senken. Dabei bleibt lediglich die Frage offen, ob sich diese Reduzierung des Spam-Anteils darauf zurückführen lässt, dass im Zusammenhang mit der Beratung technische Maßnahmen ergriffen werden oder die Mitarbeiter besser darüber aufgeklärt werden, wie sie sich von möglichen Spam-Quellen fernhalten.

Auch zeigen die Resultate einen Zusammenhang zwischen der Infektion mit Schadprogrammen in der Vergangenheit *(MalVor2004)* und dem aktuellen Anteil der Spam-Mails am gesamten E-Mail-Aufkommen. Demnach haben Unternehmen, die in den Jahren vor 2004 Opfer von Malware-Befall

gewesen sind, heutzutage fast sechs Prozent mehr Spam als Betriebe ohne Zwischenfälle in diesem Zeitraum. Ein möglicher Grund für diese Verbindung könnte sein, dass Unternehmen, die zu Beginn des neuen Jahrtausends noch nicht genügend Erfahrung mit dem Schutz vor Bedrohungen aus dem Internet gesammelt hatten, weder ausreichende Vorkehrungen gegen Malware getroffen hatten, noch genau wussten, wie sie sich im Vorfeld vor Spam-Mails schützen können. Als eine weitere Erklärungsmöglichkeit wäre auch denkbar, dass in diesem Zusammenhang das Alter einiger Unternehmen abgebildet wurde, da die Spam-Belastung nach der Einrichtung neuer E-Mail-Adressen und -Domänen im Laufe der Zeit wächst. Somit wären Unternehmen, die im Zeitraum bis 2004 noch nicht so präsent im Internet waren, in dieser Zeit sowohl einem geringeren Malware-Risiko als auch einer späteren Welle der Spam-Flut ausgesetzt gewesen.

Interessant dürfte bei dem Versuch, das individuelle Spam-Aufkommen der befragten Unternehmen zu erklären, die Überprüfung jener Variablen sein, für welche entgegen ursprünglicher Vermutungen *kein* signifikanter Zusammenhang nachgewiesen werden kann. So lässt sich beispielsweise keine Verknüpfung zwischen dem Anteil des IT-Budgets, den ein Unternehmen für IT-Sicherheit und damit auch zum Schutz vor Spam aufwendet, und der Spam-Quote am täglichen Mail-Volumen finden. Als ein möglicher Grund dafür können die kostenlos angebotenen Programme zur Spam-Filterung angesehen werden, die auch von Benutzern ohne umfangreiche IT-Kenntnisse installiert und bedient werden können.

Auch beeinflusst die Weiterbildungs- und Informationspolitik eines Unternehmens bezüglich seiner Mitarbeiter diesen Anteil nicht signifikant, so gab es zwar einen Zusammenhang dieser Variablen in der Faktorenanalyse, dieser konnte jedoch bei den Regressionen auch im bivariaten Fall nicht bestätigt werden. Demnach ergibt sich aus der Aufklärung der Anwender über unerwünschte E-Mails und deren Ursachen keine signifikante Verbesserung für die Spam-Situation dieser Firmen.

Bislang blieb die Frage, ob es sich bei den von den Unternehmen angegebenen Spam-Anteilen am Mail-Aufkommen um Werte vor oder nach der Filterung handelt, noch offen, auf Seite 125 wurden zum Vergleich die Resultate einer im gleichen Zeitraum durchgeführten Studie herangezogen. Die Frage

kann auch nach Durchführung dieser Regression nicht zweifelsfrei geklärt werden, allerdings sprechen mehrere Indizien für die These, dass es sich um ungefilterte Spam-Anteile handelt. Zwar liegen die erhobenen Werte dieser Untersuchung erheblich niedriger als jene in der 2006 durchgeführten Studie der BSI-Zeitschrift <kes>, allerdings können Unterschiede im individuellen Spam-Aufkommen nicht nur an Filtereffizienz, sondern auch an Präventivmaßnahmen und dem Verhalten im Umgang mit E-Mail-Adressen festgemacht werden. Ein weiterer Faktor, dem im Bezug auf die Spam-Vermeidung ein präventiver Charakter unterstellt werden kann, ist die IT-Beratung, die immerhin drei von fünf befragten Unternehmen nutzen.

In Bezug auf die vorliegenden Resultate sind die aufgrund ihrer Signifikanzniveaus aussagekräftigsten Koeffizienten neben der IT-Beratung sowie der Konstante die der Nutzung von E-Commerce und der Malware-Vorfälle vor 2004. Diese beiden Variablen können leicht mit unvorsichtigem Verhalten und mangelndem Gefahrenbewusstsein in Verbindung gebracht werden und bewirken beide eine deutliche Steigerung der Spam-Quote. Auch wurde bei der Interpretation des Koeffizienten zu Malware vor 2004 bereits erwähnt, dass Unternehmen, die schon länger am Internet partizipieren, auch schon länger der Belästigung durch unerwünschte E-Mails ausgesetzt sind. So haben Unternehmen, wenn sie die Online-Angebote anderer nutzen und im Zeitraum vor 2004 Probleme mit Schadprogrammen hatten, mit 35,5 % einen mehr als doppelt so hohen Spam-Anteil wie diejenigen Probanden, für welche diese beiden Eigenschaften nicht zutreffen und die sich zusätzlich noch beraten lassen.

Dieser Quotient liegt sehr nahe an den Ergebnissen der <kes>-Studie, bei welcher Mittelwert und Median um die 33 % angesiedelt waren. Gegen diese Annahme könnte lediglich der Einfluss der IT-Beratung sprechen, dieser Verbesserung kann jedoch aufgrund des geringen Wertes von sechs Prozent nicht unterstellt werden, dass sie Filtermaßnahmen zu verdanken ist, da ein solcher Filter sehr ineffizient wäre. Der beste durch das Modell erklärbare Spam-Anteil liegt entsprechend Tabelle 5.24 bei 14,2 % gegenüber der Konstante von 20,0 %, daher liegt die Vermutung nahe, dass die Teilnehmer die Frage nach dem Spam-Anteil auf Basis der ungefilterten E-Mails beantwortet haben.

5.3.4 Überlegungen zu IT-Beratung und IT-Outsourcing

Die Mehrheit der teilnehmenden Unternehmen hat im Rahmen der Studie angegeben, sich in Fragen der IT-Sicherheit von externer Seite beraten zu lassen. Viele dieser Firmen nutzen gleichzeitig die Möglichkeit, die Administration ihrer IT-Infrastruktur teilweise oder gar vollständig auszulagern, einige weitere auch ohne zusätzliche Beratung durch unternehmensfremde Experten. Insgesamt haben sich 531 der 816 Unternehmen, die sich zu diesen Fragen geäußert haben, dafür entschieden, zumindest eines dieser beiden Angebote zu nutzen und somit in dieser verantwortungsvollen Aufgabe nicht völlig auf sich allein gestellt zu sein. Diese Entscheidung geht einher mit der Bereitschaft, für eine Dienstleistung in den Bereichen Administration und IT-Sicherheit Geld an Dritte zu bezahlen, daher stellt sich die Frage, was die Unternehmen im Detail dazu veranlasst, diese Ausgaben zu tätigen.

Die Möglichkeit, sich in Fragen der IT-Sicherheit von Experten beraten zu lassen, sowie die Alternative, die Administration des IT-Bereichs teilweise oder ganz auszulagern, haben eines gemeinsam, und zwar die Inanspruchnahme externer Hilfe. Die Gründe für oder gegen einen solchen Entschluss können vielschichtig sein, doch insbesondere können sich die beiden Optionen gegenseitig bedingen. So kann sich ein Unternehmen aufgrund entsprechender Beratung dafür entscheiden, die Verantwortung für die Infrastruktur der Informationstechnologie sowie deren Absicherung gegen Bedrohungen aus dem Internet in die Hände Dritter zu legen, da es deren Fähigkeiten und Kenntnisse als besser einstuft als die eigenen. Dagegen kann Beratung aber auch dazu führen, dass ein Betrieb sich durch diese Unterstützung für die Einstellung neuer Arbeitskräfte mit entsprechendem IT-Hintergrund und daher gegen Outsourcing entscheidet.

Umgekehrt kann die Festlegung auf ein teilweises Outsourcing eine Entscheidung für Beratung nach sich ziehen, um sich für die Bereiche, die noch im eigenen Verantwortungsbereich liegen, theoretische Unterstützung zu sichern. Auch können sich Unternehmen gegen Outsourcing entscheiden, da sie es als ausreichend ansehen, sich lediglich beraten zu lassen. Häufig werden Beschlüsse zu Beratung und Outsourcing aber auch in einem Zug gefasst und nicht die Wahl einer Alternative infolge eines Entschlusses für oder gegen die

andere getroffen. So kann in einem Betrieb durchaus die Entscheidung getroffen werden, sowohl auf Beratung als auch auf Outsourcing vollständig zu verzichten, wofür es ebenfalls wieder sehr unterschiedliche Gründe geben kann. Eine solche Entscheidung muss nicht zwangsläufig auf mangelndes Problembewusstsein zurückgeführt werden, sondern kann durch eine ausreichend große Anzahl qualifizierter Leute im Unternehmen begründet sein, die sich mit angemessenen Weiterbildungsmöglichkeiten ausreichend gegen die Bedrohungen aus dem Internet gewappnet fühlen.

Aufgrund dieser Überlegungen werden in den folgenden Analysen die verschiedenen Variablen für IT-Outsourcing sowie für IT-Beratung nicht in die Regressionsmodelle aufgenommen, da hier die Kausalität nicht hinreichend geklärt werden kann. Darüber hinaus können wie schon bei der Untersuchung des Spam-Anteils die Resultate der Faktorenanalyse zurate gezogen werden, um Zusammenhänge mit bestimmten potentiellen Einflussvariablen, die nur schwach mit den zu erklärenden Variablen korreliert sind, genauer zu betrachten.

Bei den in Tabelle 5.10 bzw. 5.12 dargestellten Ergebnissen der beiden Faktorenanalysen zeigte sich neben der engen Verknüpfung mit dem Outsourcing des IT-Bereichs ein Zusammenhang zwischen IT-Beratung und der Weiterbildung von sowohl Administratoren als auch Anwendern. Auch hier ist ein kausaler Zusammenhang in einer Form, dass die Entscheidung für oder gegen Fortbildungsmaßnahmen einen Einfluss auf einen Beschluss zur Inanspruchnahme von Hilfe bei Fragen der IT-Sicherheit hat, wenig plausibel. Sinnvoller erscheint dagegen die Annahme, dass zu einem gegebenen Zeitpunkt eine Entscheidung gefällt wird, die beide Alternativen betrifft, aus dieser Überlegung heraus wurden die verschiedenen Facetten der Weiterbildungsmöglichkeiten nicht in das Regressionsmodell einbezogen.

Eine Abhängigkeit der Entscheidung für oder gegen das Suchen von Unterstützung im Bereich IT-Sicherheit vom Anteil der IT-Fachkräfte auf der einen und vom Anteil der Administratoren am Personalbestand auf der anderen Seite ergibt dagegen einen Sinn. Je mehr ausgebildetes Personal einem Unternehmen zur Bewältigung der Probleme der IT-Sicherheit zur Verfügung steht, desto eher könnte es sich zu einem Verzicht auf die Hilfe einer Consulting-Firma entschließen.

IT-Beratung	**schrittw.**	**Std. Abw.**
AntIT	-0,0037***	0,0007
AntSumAI	-0,0030**	0,0013
MalNein (b)	-0,0744*	0,0383
AntITS0105 (b)	-0,0825**	0,0381
Anz. Beob.	664	
Pseudo-R^2	0,0573	
Log Likelihood	-405,6	

Erklärung: ***Signifikanz zum 1 %-Niveau, **Signif. zum 5 %-Niveau, *Signif. zum 10 %-Niveau, (b) binäre Variable

Tabelle 5.25: Logit-Schätzung der IT-Beratung

Dass diese Abhängigkeiten signifikant sind, geht aus Tabelle 5.25 hervor, so steigt die Chance für eine Entscheidung zugunsten von IT-Beratung, je weniger Personal mit IT-Ausbildung oder -Studium *(AntIT)* ein Betrieb beschäftigt. Ähnlich sieht es beim Anteil der Administratoren *(AntSumAI)* aus, auch wenn hier der Effekt etwas geringer ausfällt und weniger signifikant ist, Einsparungen an IT-Personal infolge von Beratung erscheint hingegen weniger sinnvoll.

Signifikant seltener Ratschläge zur IT-Sicherheit lassen sich diejenigen Unternehmen geben, die maximal fünf Prozent ihres IT-Budgets für IT-Sicherheit aufbringen *(AntITS0105).* Das heißt, dass Firmen mit geringerer Investitionsbereitschaft in IT-Sicherheit auch mit einer um acht Prozent höheren Wahrscheinlichkeit keine Mittel für IT-Beratung zur Verfügung stellen als andere Unternehmen.

Des Weiteren stützen sich all jene Betriebe, die bislang noch keine Vorfälle durch Schadprogramme zu beklagen hatten *(MalNein),* seltener auf die Erfahrung Dritter. Dieser Zusammenhang ist einfach nachvollziehbar, da hier aufgrund eines erfolgreichen Konzepts zum Schutz vor Bedrohungen aus dem Internet offenbar kein Bedarf an Unterstützung im Kampf gegen Malware besteht.

Zusammenfassend kann festgestellt werden, dass IT-Beratung häufig bei jenen Unternehmen vorzufinden ist, die bereits Vorfälle durch Malware und damit durch Schadprogramme verursachte Kosten zu tragen hatten. Diese Kosten sollen durch Consulting im Bereich der IT-Sicherheit gesenkt werden,

komplettes IT-Outsourcing	**schrittw.**	**Std. Abw.**
AnzMA	-0,0007***	0,0001
B2CAnt	-0,0019*	0,0011
Anz. Beob.	729	
Pseudo-R^2	0,0404	
Log Likelihood	-296,8	

Erklärung: ***Signifikanz zum 1 %-Niveau, *Signifikanz zum 10 %-Niveau, (b) binäre Variable

Tabelle 5.26: Logit-Schätzung des kompletten IT-Outsourcings

insbesondere wenn diesem Problem nicht durch einen ausreichend großen und qualifizierten Personalanteil entgegengewirkt werden kann.

Gab es bei der Untersuchung der Wahrscheinlichkeiten für Probleme mit Malware oder Spam keine signifikanten Unterschiede für die Unternehmensgröße, so treten diese nun bei der Entscheidung für das komplette Outsourcing der Administration in Erscheinung. Demnach sinkt laut Tabelle 5.26 mit wachsendem Personalbestand eines Betriebs *(AnzMA)* die Wahrscheinlichkeit der vollständigen Auslagerung des IT-Bereichs, da für große Unternehmen das Betreiben einer eigenen IT-Abteilung rentabler sein dürfte als für kleine und mittlere Betriebe. Dagegen könnte selbst die Einstellung eines Mitarbeiters ausschließlich zur Administration der IT-Infrastruktur für kleinere Firmen zu teuer und damit nicht realisierbar sein.

Ein größerer Anteil des E-Commerce am jährlichen Umsatz *(B2CAnt)* beeinflusst die Entscheidung zum kompletten Outsourcing negativ, demnach möchten Unternehmen mit steigender Abhängigkeit vom E-Commerce die Administration ihres IT-Bereichs nicht komplett aus der Hand geben. Im Gegenzug wächst gemäß Tabelle 5.27 mit einem zunehmendem Umsatzanteil durch E-Commerce die Entscheidung zum Verzicht auf jegliche Auslagerung der IT-Verantwortung. Eine Verknüpfung mit dem teilweisen Outsourcing hingegen erwies sich als insignifikant, ebenso wie alle in ihrer Kausalität eindeutigen Zusammenhänge zwischen dem teilweisen Outsourcing und anderen Variablen zu insignifikanten Ergebnissen führten. Demnach verlassen sich Unternehmen, für welche der Online-Handel eine wichtige Einnahmequelle ist, bei der Administration ihrer IT-Anlagen lieber auf die eigenen Fähigkeiten.

Verzicht auf IT-Outsourcing	**schrittw.**	**Std. Abw.**
B2CAnt	0,0030*	0,0016
WBAdmin (b)	0,2612***	0,0354
MalNein (b)	0,0699*	0,0378
Anz. Beob.	724	
Pseudo-R^2	0,0598	
Log Likelihood	-460,5	

Erklärung: ***Signifikanz zum 1 %-Niveau, *Signifikanz zum 10 %-Niveau, (b) binäre Variable

Tabelle 5.27: Logit-Schätzung des Verzichts auf IT-Outsourcing

Auch zeigt sich beim Verzicht auf das Auslagern von IT-Verantwortung, dass Unternehmen, bei denen es noch nie zu Malware-Befall gekommen ist, wie bei der Beratung auch die Möglichkeit des Outsourcings nicht in Anspruch nehmen. Wie schon bei der Beratung zur IT-Sicherheit liegt auch beim IT-Outsourcing die Wahrscheinlichkeit für Unternehmen, die in Bezug auf Viren, Würmer und Trojaner eine weiße Weste haben, um sieben Prozent niedriger. Zu guter Letzt entscheiden sich Firmen, die ihren Administratoren eine Weiterbildung *(WBAdmin)* ermöglichen, mit 26 % erheblich häufiger gegen die Abtretung der IT-Verantwortung an Drittunternehmen.

Die Betrachtung der Voraussetzungen für Beratung zu IT-Sicherheit und für IT-Outsourcing hat gezeigt, dass Unternehmen sich unter bestimmten Umständen dazu entschließen, andere Unternehmen, die sich auf Administration und IT-Sicherheit spezialisiert haben, für eben diese Aufgaben zu beauftragen. Dies geschieht mit einer um sieben Prozent höheren Wahrscheinlichkeit bei Firmen, die bereits Vorfälle durch Schadprogramme und damit vermeidbare Kosten gehabt haben, auch hatten diese Unternehmen in der Umfrage signifikant höhere Zahlungsbereitschaften für die betrachteten Aspekte der IT-Sicherheit geäußert. Die Aufwendungen für die Fremdvergabe dieser Aufgaben können jedoch auch in die Qualifikation der eigenen Mitarbeiter investiert werden oder in Form von höheren Gehältern bei der Einstellung von IT-Experten sinnvoller angelegt werden. Fakt ist, dass Unternehmen vor Allem dann zu Ausgaben für IT-Sicherheit bereit sind, wenn sie von dieser in besonderem Maße abhängig sind.

Kapitel 6

Schlussbemerkungen

Als John von Neumann im Jahre 1949 zum ersten Mal den Gedanken von sich selbst reproduzierenden Automaten ins Auge fasste, konnte er noch nicht ahnen, dass die praktische Umsetzung seines theoretischen Konzepts einmal mitten im Blickfeld kriminalpolizeilicher Ermittlungsbehörden stehen würde. So stand die Herbsttagung 2007 des deutschen Bundeskriminalamts unter dem Motto „Tatort Internet – eine globale Herausforderung für die Innere Sicherheit“ und thematisierte dort neben Kinderpornographie und Terrorismus auch die Probleme der IT-Sicherheit.

Während Experten die ersten Versuche mit selbst replizierenden Computerprogrammen in den 70ern noch interessiert beobachteten, wurde das Phänomen in den 80ern bereits kritisch beäugt, wiederholte Vorfälle mit Schadprogrammen in den 90ern machten deutlich, dass das Problem gut im Auge behalten werden musste. Spätestens seit Erscheinen der Meldung *„I love you“* blickt die ganze Computerwelt gebannt auf weitere Meldungen über globale Malware-Epidemien und hält nach Lösungen für die Beseitigung dieser Gefahr für die IT-Sicherheit Ausschau.

Der in Kapitel 2 gegebene Überblick über IT-Sicherheit hat gezeigt, dass die Gewährleistung derselben wichtig ist, um die Vertraulichkeit und Verfügbarkeit sowie die Integrität von Daten und Diensten gewährleisten zu können. So stellen Schadprogramme gemäß der <kes>-Studie (2006a) – neben dem technischen Unvermögen von Benutzern – mit die größte Bedrohung für diese drei Säulen der IT-Sicherheit dar und machen einen guten und umfassenden

Schutz vor diesen Gefahren aus dem Internet unumgänglich. Doch nicht nur die Maßnahmen zur Verhinderung von Malware-Befall von Computern kosten Geld, auch durch die Infektion mit Schadprogrammen entstehen Kosten, die oft nur schwer quantifiziert werden können. Eine ungefähre Abschätzung der Kosten, die durch Malware verursacht werden, war eines der vornehmlichen Ziele der vorliegenden Arbeit.

Neben dem Kampf gegen Viren, Würmer und Trojaner, der alljährlich immense Geldbeträge verschlingt, verursachen auch die Maßnahmen gegen unerwünschte E-Mails beträchtliche Kosten, insbesondere dann, wenn sie nicht ausreichen, um der Spam-Flut Herr zu werden. Waren Spam-Mails zu Beginn noch ein störendes Element des Internets, so stellen sie in der Zwischenzeit eine ernstzunehmende Gefahr für Mail-Server und Mail-Provider dar, eine Bedrohungslage, die nicht zuletzt durch die Entstehung von Botnetzen entstanden ist. Auch kostet das manuelle Löschen oder gar Lesen der Nachrichten unnötig Zeit und zieht damit enorme Kosten nach sich, deren Untersuchung sich auch nach Meinung von Clement et al. (2008) in Zukunft mehr Wissenschaftler widmen sollten.

Auf der in Kapitel 3 dokumentierten Suche nach einer geeigneten Methode zur Quantifizierung der Kosten, welche durch Schadprogramme und unerwünschte E-Mails verursacht werden, fiel die Entscheidung auf die *Contingent Valuation* Methode. Dieses präferenzbasierte Verfahren wurde verschiedenen kennzahlenbasierten Ansätzen zur Schätzung von Kosten vorgezogen, obwohl letztere in der Praxis zur Anwendung kommen und teilweise auch zur Berechnung der Kosten von IT-Sicherheit herangezogen werden. Dagegen fand die CVM bislang schwerpunktmäßig im Bereich der Umwelt- und Ressourcenökonomik Verwendung, vor wenigen Jahren wurde sie auch erstmals bei der Schätzung der Kosten von (Gewalt-)Kriminalität eingesetzt und führte dort zu Ergebnissen, welche dem Vergleich mit anderen Schätzansätzen standhalten konnten. Der bereits erfolgte Einsatz der *Contingent Valuation* im Bereich der Kriminometrie sowie ihre Flexibilität machten das Verfahren für die Schätzung der Kosten von Malware und Spam unter Beachtung gewisser Voraussetzungen attraktiv, da die Methode häufig bei der Berechnung von Kosten zum Einsatz kommt, wenn für die zu bewertenden Güter keine Marktpreise existieren – wie es oft bei öffentlichen Gütern der Fall ist.

Die einzelnen Schritte bei der Entwicklung des Fragebogens der CV-Studie, welche in Zusammenarbeit mit dem ZEW durchgeführt wurde, werden in Kapitel 4 wiedergegeben, dabei wurden die Vorgaben der NOAA-Kommission bestmöglich im Design der Studie berücksichtigt. Ziel der Befragung war, eine Zahlungsbereitschaft der Unternehmen des IKT-Dienstleistungssektors für die Reduzierung des Malware-Aufkommens sowie der Reduzierung des Spam-Anteils zu erheben, mit welcher dann die Kosten geschätzt werden können, die jenen Unternehmen durch die beiden Phänomene der Internet-Kriminalität entstehen.

Aus der Untersuchung der so erhobenen Umfragedaten in Kapitel 5 ergab sich unter Anderem, dass nur die Hälfte der befragten Unternehmen zu Protokoll gab, in den vergangenen Jahren Opfer von Malware-Vorfällen gewesen zu sein. Dabei traf es jene Unternehmen, die Probleme zu beklagen hatten, häufig nicht nur in einem der beobachteten Jahre bzw. Zeiträume, vielmehr wurde fast jeder fünfte Teilnehmer in dieser Zeit wiederholt Opfer von Viren, Würmern oder Trojanern. Auch lag der Spam-Anteil am gesamten Mail-Aufkommen bei den IKT-nahen Dienstleistern überraschend niedrig, für diese beiden Phänomene wurden andere Studien zum Vergleich herangezogen, in denen ein erheblich größerer Anteil der Teilnehmer Opfer von Malware geworden war bzw. mit einem deutlich höheren Spam-Aufkommen zu kämpfen hatte.

Ein effektiver Schutz gegen diese beiden Facetten der Internet-Kriminalität ist demnach möglich, insbesondere bei den Mitgliedern des Wirtschaftszweiges „Software und IT-Dienste“ gab es bei nicht einmal einem Drittel der Firmen Vorfälle durch Schadprogramme und die Mehrheit der Unternehmen hat nur bis zu zehn Prozent Spam-Anteil. Des Weiteren zeigen die Resultate, dass im Zusammenhang mit Malware die Opferrolle nicht ganz zufällig verteilt ist, vielmehr scheint es mit 36 % der insgesamt betroffenen Unternehmen immer wieder die gleichen zu treffen. Auch führen bestimmte Verhaltensmuster wie die Teilnahme am elektronischen Handelsverkehr zu signifikant mehr unerwünschten E-Mails.

Neben der Identifikation solcher Zusammenhänge zwischen Malware-Infektionen und den Ursachen für das unternehmensspezifische Spam-Aufkommen war die Schätzung der Kosten, welche durch diese beiden Bedrohungen aus

dem Internet verursacht werden, eines der grundlegenden Ziele der *Contingent Valuation*-Studie. Dabei wurde festgestellt, dass die von den Unternehmen geäußerten Zahlungsbereitschaften hauptsächlich von der Mitarbeiterzahl abhängig waren, nicht hingegen von ihren Umsatzzahlen. Erwartungsgemäß nahm dabei die individuell wahrgenommene Bedrohungssituation durch Schadprogramme respektive die Störung durch unerwünschte E-Mails signifikant Einfluss auf die *Willingness to pay* der Teilnehmer in Relation zu ihrem jeweiligen Personalbestand.

Analog zu den Schätzungen von Ludwig und Cook (2001) sowie Cohen et al. (2004) für eine theoretische hundertprozentige Senkung der betrachteten Kriminalitätskategorien würden den befragten Unternehmen Kosten von ungefähr 100 Euro pro Mitarbeiter durch Malware bzw. 50 Euro durch Spam entstehen. Bei einer Hochrechnung dieser betriebswirtschaftlichen Kosten auf die etwas mehr als 2,2 Mio. Beschäftigten der beobachteten Wirtschaftszweige unter Annahme der Repräsentativität würden demnach den Unternehmen Kosten von jährlich insgesamt 222 Mio. Euro durch Schadprogramme sowie 111 Mio. Euro durch unerwünschte E-Mails entstehen. Dieser immense Schaden bezieht sich jedoch nur auf die Dienstleister der IKT-Branche, die einerseits durch ihre Nähe zur Informationstechnologie besser geschützt zu sein scheinen, andererseits jedoch auch in einem viel größeren Ausmaß von deren Zuverlässigkeit abhängig sein dürften.

Sollen nun die Schätzergebnisse, welche für die Dienstleister der Informationsgesellschaft entwickelt wurden, auf alle Beschäftigten des Erhebungsjahres 2006 hochgerechnet werden, so ist zu beachten, dass die Resultate der betrachteten Branche nicht repräsentativ für die anderen Wirtschaftszweige sind. Die Statistischen Ämter des Bundes und der Länder (2009) beziffern die Zahl der Beschäftigten in Deutschland für das Jahr 2006 auf 39,1 Millionen, von denen nach Angaben des Bundesverbandes Informationswirtschaft, Telekommunikation und neue Medien e.V. (BITKOM, 2007) in jenem Jahr 56 % beruflich an einem Computer arbeiteten.[1] Wird diese Quote in Relation zum Anteil der Mitarbeiter mit Computer am Arbeitsplatz von 77 % in der IKT-Branche gesetzt, so ergibt sich ein Korrekturfaktor von ungefähr 0,73.

[1] Zur Erhebung dieses Wertes wurden Unternehmen mit mindestens zehn Beschäftigten befragt, der Bankensektor war nach Angabe des Branchenverbandes ausgenommen.

Die Berücksichtigung dieses Faktors ist notwendig, um die Resultate unter Einbeziehung der abweichenden Arbeitsbedingungen der Branche der IT-nahen Dienstleister zumindest teilweise auf die anderen Wirtschaftssektoren abbilden zu können. Soll also anhand der erhobenen Zahlungsbereitschaften das Kostenpotential von Schadprogrammen bzw. von unerwünschten E-Mails für alle Beschäftigten in Deutschland geschätzt werden, so kann dieser Schritt nur dann zulässig sein, wenn die branchenbezogenen Ergebnisse durch den Faktor korrigiert werden.

Unter der Annahme, dass die hier erläuterten Schlussfolgerungen ausreichend sind, um repräsentativ für alle Branchen zu sein, ergäbe sich somit für Viren, Würmer und Trojaner ein Kostenpotential von 2,84 Mrd. Euro. Dementsprechend beliefen sich die Kosten, welche durch unerwünschte E-Mails verursacht werden, auf 1,42 Mrd. Euro. Analog zu den Berechnungen auf Seite 152 handelt es sich auch bei den hier genannten Werten nur um eine untere Schranke, es kann davon ausgegangen werden, dass die tatsächlichen Kosten, welche jährlich durch Schadprogramme sowie durch Spam-Mails verursacht werden, erheblich höher sind. Wie eingangs erläutert gibt es jedoch bereits zu viele Studien, welche mit möglichst hohen Kosten Aufmerksamkeit erregen wollten, deren Berechnungen hingegen aus wissenschaftlicher Sicht nicht haltbar sind. Aus diesem Grund wurden in dieser Arbeit mit der unteren Schranke nur die minimalen Kostenpotentiale angegeben.

Dennoch geben die Resultate einen Vorgeschmack dessen, was diese beiden Phänomene der Kriminalität im Internet in anderen Branchen, bei wissenschaftlichen Einrichtungen, in der Verwaltung, und nicht zuletzt bei jedem einzelnen Bürger an Kosten verursachen können. Daher ist die Gewährleistung der IT-Sicherheit durch präventive Maßnahmen ein wichtiges Mittel, um Aufwendungen für korrektive Maßnahmen zur Beseitigung von Malware und zur Wiederherstellung der IT-Sicherheit zu vermeiden. Diese Kosten sind bedingt durch Ausfallzeiten und damit zusammenhängende Produktivitätsverluste erheblich größer als der finanzielle Aufwand für Investitionen in die IT-Sicherheit. Dennoch liegt bei fast jedem zweiten Teilnehmer der vorliegenden Studie der Anteil für IT-Sicherheit am IT-Budget bei maximal fünf Prozent, laut FAZIT-Umfrage (2005) sind es bei den anderen Unternehmen sogar mehr als die Hälfte.

In unserer Gesellschaft sind Haustüren eine völlig alltägliche Erscheinung, sie können verschlossen werden, um sowohl bei An- als auch bei Abwesenheit Fremde am Betreten einer Wohnung oder eines Gebäudes zu hindern. Sie stellen eine Zugangskontrolle dar, welche von Privatpersonen und von Unternehmen gleichermaßen wie selbstverständlich eingesetzt wird, die Umsetzung dieses Konzepts auf den virtuellen Raum ist jedoch noch nicht überallhin durchgedrungen. Teilweise stellen auch extrem einfache Passwörter eine angreifbare Lücke in einem sonst gut durchdachten Sicherheitskonzept dar, denn was hilft ein Sicherheitsschloss in einer einbruchsicheren Tür, wenn der Schlüssel unter der Fußmatte liegt?

Die im Rahmen dieser Arbeit entwickelten Überlegungen sowie ihre Resultate sollten als starkes Argument dafür dienen, nicht nur Computer, sondern jegliche Form von technischen Geräten, die von Schadsoftware betroffen sein können, entsprechend gegen Malware zu schützen. Auch sollen die Resultate als Aufruf verstanden werden, alle Personen, die mit ihrem Computer eine Verbindung zu anderen Rechnern aufbauen, über die Gefahren aufzuklären, die im Internet lauern. Anbieter von E-Mail-Diensten haben hier ihre Verantwortung bereits erkannt, nicht zuletzt um sich auch selbst durch die Aufklärung ihrer Kunden zu schützen. Auch informieren Kreditinstitute, die Online-Banking anbieten, ihre Kunden darüber, wie sie durch das Erkennen von Phishing-Mails verhindern können, das Opfer von Online-Betrügern zu werden.

IT-Sicherheit geht uns alle etwas an und sollte als wichtige Grundlage unserer Informationsgesellschaft erkannt werden, auch sollte sich jeder Teilnehmer am weltweiten Datennetz seiner eigenen Verantwortung bewusst sein, welche er durch seine Partizipation im Internet auf sich nehmen muss. Beim Kampf gegen Malware und Spam auf die Anstrengungen anderer zu hoffen, kann dabei nicht der richtige Weg sein, es darf also nicht heißen „Es muss etwas geschehen“, sondern „Wir müssen etwas tun“.

Literaturverzeichnis

[AT03] Abel, C. und R. Thiele (2003). ROSI – mehr Schein als Sein?! – Warum es so schwer ist, IT Sicherheit zu rechtfertigen. Whitepaper DMR Consulting GmbH.

[AS+93] Arrow, K., R. Solow, P. R. Portney, E. E. Leamer, R. Radner und H. Schuman (1993). Report of the NOAA Panel on Contingent Valuation. *Federal Register 58* (January 15), S. 4601-4614.

[BE+06] Backhaus, K., B. Erichson, W. Plinke und R. Weiber (Hrsg.) (2006). *Multivariate Analysemethoden: Eine anwendungsorientierte Einführung.* (11. Auflage). Berlin, Heidelberg: Springer.

[B93] Becker, G. S. (1993). Nobel Lecture: The Economic Way of Looking at Behavior. *Journal of Political Economy 101* (3), S. 385-409.

[BO05] Bertschek, I. und J. Ohnemus (2005). Open Source Software und IT-Sicherheit: Ergebnisse der ersten FAZIT-Unternehmensbefragung. In I. Bertschek und T. Döbler (Hrsg.). *Open Source Software und IT-Sicherheit. FAZIT-Schriftenreihe, Forschungsbericht Bd. 1.* S. 15-60. Stuttgart.

[B07] Bitkom (o. V.) (2007). Daten zur Informationsgesellschaft. PDF-Datei online verfügbar unter `http://www.bitkom.org/files/documents/Daten_zur_Informationsgesellschaft_2007.pdf` (Stand: 20.07.2009).

[BSI07] Bundesamt für Sicherheit in der Informationstechnik (o. V.) (2007). Leitfaden IT-Sicherheit. PDF-Datei online verfügbar

unter http://www.bsi.de/gshb/Leitfaden/GS-Leitfaden.pdf (Stand: 20.07.2009).

[BSI09] Bundesamt für Sicherheit in der Informationstechnik (o. V.) (2009). BSI für Bürger. HTML-Datei online verfügbar unter http://www.bsi-fuer-buerger.de/ (Stand: 20.07.2009).

[PKS99] Bundeskriminalamt (o. V.) (1999). Polizeiliche Kriminalstatistik 1998. Wiesbaden.

[PKS00] Bundeskriminalamt (o. V.) (2000). Polizeiliche Kriminalstatistik 1999. Wiesbaden.

[PKS01] Bundeskriminalamt (o. V.) (2001). Polizeiliche Kriminalstatistik 2000. Wiesbaden.

[PKS02] Bundeskriminalamt (o. V.) (2002). Polizeiliche Kriminalstatistik 2001. Wiesbaden.

[PKS03] Bundeskriminalamt (o. V.) (2003). Polizeiliche Kriminalstatistik 2002. Wiesbaden.

[PKS04] Bundeskriminalamt (o. V.) (2004). Polizeiliche Kriminalstatistik 2003. Wiesbaden.

[PKS05] Bundeskriminalamt (o. V.) (2005). Polizeiliche Kriminalstatistik 2004. Wiesbaden.

[PKS06] Bundeskriminalamt (o. V.) (2006). Polizeiliche Kriminalstatistik 2005. Wiesbaden.

[PKS07] Bundeskriminalamt (o. V.) (2007). Polizeiliche Kriminalstatistik 2006. Wiesbaden.

[PKS08] Bundeskriminalamt (o. V.) (2008). Polizeiliche Kriminalstatistik 2007. Wiesbaden.

[EPS01] Bundesministerium des Innern, Bundesministerium der Justiz (o. V.) (2001). Erster Periodischer Sicherheitsbericht (Tech. Rep.). Berlin.

[ZPS06] Bundesministerium des Innern, Bundesministerium der Justiz (o. V.) (2006). Zweiter Periodischer Sicherheitsbericht (Tech. Rep.). Berlin.

[CM+92] Carson, R., R. C. Mitchell, W. M. Hanemann, R. J.,Kopp, S. Presser und P. A. Ruud (1992). A Contingent Valuation Study of Lost Passive Use Values Resulting From the Exxon Valdez Oil Spill. Report to the Attorney General of the State of Alaska.

[C94] Carson, R. (1994). Contingent Valuation Surveys and Test of Insensitivity to Scope. Vortrag im Rahmen der International Conference on Determining the Value of Non-marketed Goods: Economic Psychological, and Policy Relevant Aspects of Contingent Valuation Methods. Bad Homburg (Deutschland), Juli 1994.

[C+94a] Carson, R., J. Wright, A. Alberini, N. Carson und N. Flores (1994). A Bibliography of Contingent Valuation Studies and Papers. La Jolla, CA: Natural Resource Damage Assessment Inc.

[C+94b] Carson, R. T., N. E. Flores, K. Martin und J. Wright (1994). Contingent Valuation and Revealed Preference Methodologies: Comparing the Estimates for Quasi-Public Goods. Discussion Paper 94-07. University of California, San Diego.

[CM95] Carson, R. und R. Mitchell (1995). Sequencing and Nesting in Contingent Valuation Surveys. *Journal of Environmental Economics and Management 28*, S. 155-173.

[CFH98] Carson, R., N. E. Flores und W. M. Hanemann (1998). Sequencing and Valuing Public Goods. *Journal of Environmental Economics and Management 36*, S. 314-324.

[C00] Carson, R. (2000). Contingent Valuation: A User's Guide. *Environmental Science & Technology 34* (8), S. 1413-1418.

[CBS04] CBS NEWS (o. V.) (2004). Gates: Spam To Be Canned By 2006 – Microsoft Chairman Announces Plans To End Junk

E-Mail. HTML-Datei online verfügbar unter `http://www.cbsnews.com/stories/2004/01/24/tech/main595595.shtml` (Stand: 20.07.2009, Veröffentlichung: 24.01.2004).

[C47] Ciriacy-Wantrup, S. V. (1947). Capital Returns from Soil Conservation Practices. *Journal of Farm Economics 29*, S. 1181-1196.

[CPB08] Clement, M., D. Papies und H. J. Boie (2008). Kosten und Kostentreiber von unerwünschten Werbemails (Spam) – Eine empirische Analyse auf Provider- und Anwenderseite. Zeitschrift für Betriebswirtschaft *Zeitschrift für Betriebswirtschaft 78* (4), S. 339-366.

[C84] Cohen, F. (1984). Computer Viruses – Theory and Experiments. HTML-Datei online verfügbar unter `http://all.net/books/virus/index.html` (Stand: 20.07.2009)

[CR+04] Cohen, M. A., R. T. Rust, S. Steen und S. T. Tidd (2004). Willingness-to-Pay for Crime Control Programs. *Criminology 42* (1), S. 89-109.

[C01] Computerwoche.de (o. V.) (2001). „Code-Red"-Bilanz: 2,6 Milliarden Dollar Schaden. `http://www.computerwoche.de/nachrichten/523205` (Stand: 20.07.2009, Veröffentlichung: 03.09.2001).

[CA98] Cropper, M. und A. Alberini (1998). Contingent Valuation In P. Newman (Ed.). *The New Palgrave Dictionary of Economics and the Law*, S. 558-575. New York: Stockton Press.

[CS07] CTO STRATO Rechenzentrum AG (R. Wienholtz) (2007). Phishing, Pharming, and Phraud: The Joy of Phighting Email Spam. Vortrag im Rahmen des 5th German Anti-Spam Summit. Köln (Deutschland), 5. September 2007. PDF-Datei online verfügbar unter `http://www.eco.de/dokumente/10_Strato_RWienholtz_5dask2007.pdf` (Stand: 20.07.2009).

[D63] Davis, R. (1963). The Value of Outdoor Recreation: An Economic Study of the Maine Woods. Unpublished doctoral dissertation. Harvard University.

[DH+93] Diamond, P. A., J. A. Hausman, G. K. Leonard und M. A. Denning (1993). Does Contingent Valuation Measure Preferences? Experimental Evidence. In J. A. Hausman (Ed.). *Contingent Valuation: A Critical Assessment*, S. 41-89. New York: North-Holland Press.

[DH94] Diamond, P. A. und J. A. Hausman (1994). Contingent Valuation: Is Some Number Better than No Number? *Journal of Economic Perspectives 8* (4), S. 45-64.

[D92] DiBona, C. J. (1992). Assessing Environmental Damage. *Issues in Science and Technology 8*, S. 50-54.

[El07] eleven GmbH (R. Rothe) (2007). Spam: a mere nuisance evolving into a massive threat to infrastructure and communication – Latest figures and statistics, development and consequences. Vortrag im Rahmen des 5th German Anti-Spam Summit. Köln (Deutschland), 5. September 2007. PDF-Datei online verfügbar unter `http://www.eco.de/dokumente/1_eleven_5dask2007.pdf` (Stand: 20.07.2009).

[En07] ENISA – European Network and Information Security Agency (P. Manzano und C. Rossow) (2007). Result from ENISA 2007 survey on providers' security and anti-spam measures. Vortrag im Rahmen des 5th German Anti-Spam Summit. Köln (Deutschland), 5. September 2007. PDF-Datei online verfügbar unter `http://www.eco.de/dokumente/3_ENISA_PManzano_5dask2007.pdf` (Stand: 20.07.2009).

[FTC05] Federal Trade Commission (S. Wernikoff) (2005). Federal Trade Commission: Actions and Campaigns. Vortrag im Rahmen des 3rd German Anti-Spam Summit. Köln (Deutschland), 7. September 2005.

[FTC07] Federal Trade Commission (o. V.) (2007). Spam Summit: The Next Generation of Threats and Solutions. PDF-Datei online verfügbar unter `http://www.ftc.gov/os/2007/12/071220spamsummitreport.pdf` (Stand: 20.07.2009, Veröffentlichung: 20.12.2007).

[F04] Frank, T. (2004). Zur strafrechtlichen Bewältigung des Spamming. Kognos Verlag, Berlin. ISBN 3-8325-0491-5.

[UWG] Gesetz gegen den unlauteren Wettbewerb (o. V.) (2009). PDF-Dokument online verfügbar unter `http://www.gesetze-im-internet.de/bundesrecht/uwg_2004/gesamt.pdf` (Stand: 20.07.2009)

[G05] Greenpeace (o. V.) (2009). Exxon Valdez Katastrophe – 16 Jahre später. HTML-Datei online verfügbar unter `http://www.greenpeace.de/themen/oel/oeltanker/artikel/exxon_valdez_katastrophe_16_jahre_spaeter/` (Stand: 20.07.2009, Veröffentlichung: 17.03.2005).

[HG99] Hammit, J. K. und J. D. Graham (1999). Willingness to Pay for Health Protection: Inadequate Sensitivity to Probability? *Journal of Risk and Uncertainty 8*, S. 33-62.

[H94] Hanemann, W. M. (1994). Valuing the Environment Through Contingent Valuation. *Journal of Economic Perspectives 8* (4), S. 19-43.

[H07] heise online (Autor: D. Knop) (2007). Sturm-Wurm-Botnetz mit über 1,7 Millionen Drohnen. `http://www.heise.de/newsticker/meldung/94016` (Stand: 20.07.2009, Veröffentlichung: 08.08.2007).

[I07] Internet Crime Complaint Center (o. V.) (2007). Internet Crime Report 2006. PDF-Datei online verfügbar unter `http://www.ic3.gov/media/annualreport/2006_IC3Report.pdf` (Stand: 20.07. 2009, Veröffentlichung: 2007).

[I06] IronPort Systems (A. Kraus) (2006). Spammers Continue Innovation: Image-based Spam and Bounce Attacks are the latest Inbox Threats. Vortrag im Rahmen des 4th German Anti-Spam Summit. Köln (Deutschland), 5. September 2006.

[JT08] Joseph, K. und A. Thevaranjan (2008). Investigating Pricing Solutions to Combat Spam: Postage Stamp and Bonded Senders. Erscheint in: Journal of Interactive Marketing.

[KK92] Kahneman, D. und J. L. Knetsch (1992). Valuing Public Goods: The Purchase of Moral Satisfaction. *Journal of Environmental Economics and Management 22*, S. 57-70.

[K99] Kaiser, U. (1999). Die ZEW/Creditreform Konjunkturumfrage bei unternehmensnahen Dienstleistern. *Allgemeines Statistisches Archiv (Rundschau) 83*, S. 447-451.

[KH03] Kaspersky (o. V.) (2003). Viruslist.com – History of Malicious Programs. HTML-Datei online verfügbar unter `http://www.viruslist.com/en/viruses/encyclopedia?chapter=153280684` (Stand: 20.07.2009, letztes Berichtsjahr 2003).

[KES06a] <kes> Die Zeitschrift für Informations-Sicherheit (2006a). Lagebericht zur Informations-Sicherheit. *<kes> – Zeitschrift für Kommunikations- und EDV-Sicherheit Nr. 4*, August/September, S. 24-31. SecuMedia Verlag, Ingelheim.

[KES06b] <kes> Die Zeitschrift für Informations-Sicherheit (2006b). Lagebericht zur Informations-Sicherheit (3). *<kes> – Zeitschrift für Kommunikations- und EDV-Sicherheit Nr. 6*, Dezember, S. 48-60. SecuMedia Verlag, Ingelheim.

[KM00] King, D. M. und M. Mazzotta (2000). Ecosystem Valuation. HTML-Datei online verfügbar unter `http://www.ecosystemvaluation.org/contingent_valuation.htm` (Stand: 20.07.2009, letzte Änderung: 01.09.2000).

[KD66] Knetsch, J. L. und R. K. Davis (1966). Comparisons of Methods for Recreation Evaluation. In A. V. Kneese und S. C. Smith (Eds.). *Water Research*, S. 125-142. Baltimore: Resources for the Future Inc., Johns Hopkins Press.

[KEU04] Kommission der Europäischen Gemeinschaften (o. V.) (2004). Mitteilung der Kommission an das europäische Parlament, den Rat, den europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen über unerbetene Werbenachrichten (Spam). PDF-Dokument online verfügbar unter `http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2004:0028:FIN:DE:PDF` (Stand: 20.07.2009).

[K67] Krutilla, J. (1967). Conservation Reconsidered. *American Economic Review 56*, S. 777-786.

[LKA05] Landeskriminalamt Baden-Württemberg (F. Eißmann) (2005). Internationale Zusammenarbeit der Strafverfolgungsbehörden gegen Botnetze und Trojaner. Vortrag im Rahmen des 3rd German Anti-Spam Summit. Köln (Deutschland), 8. September 2005.

[LC01] Ludwig, J. und P. J. Cook (2001). The Benefits of Reducing Gun Violence: Evidence from Contingent-Valuation Survey Data. *International Review of Law and Economics 22* (3), S. 207-226.

[MAA05] MAAWG – Messaging Anti-Abuse Working Group (B. Roth) (2005). Ohne Titel. Vortrag im Rahmen des 3rd German Anti-Spam Summit. Köln (Deutschland), 7. September 2005.

[MS04] Microsoft Präsentation von Baumann, U. und D. Primbs (2004). Viren, Würmer, SP2. PPT-Dokument online verfügbar unter `http://download.microsoft.com/downlaod/7/b/f/7bf209e7-d933-4c6f-a768-0f01f3e7cf98/VirenTechTalk.ppt` (Stand: 20.07.2009, Veröffentlichung: 2004).

[MS05] Microsoft/MSN (D. Finn) (2005). Prosecution by Microsoft/MSN in the U.S. and Europe. Vortrag im Rahmen des 3rd German Anti-Spam Summit. Köln (Deutschland), 8. September 2005.

[MC89] Mitchell, R. und R. Carson (1989). Using Surveys to Value Public Goods: The Contingent Valuation Method. Washington, D.C.: Resources for the Future.

[MC03] Mummert Consulting (o. V.) (2003). IT-Security 2003: ROSI hilft sparen. HTML-Datei war online verfügbar unter `http://www.systems-world.com/link/de/17162343` (Stand: 02.03.2008, Veröffentlichung: 2003).

[N01a] Nagin, D. S. (2001a). Costs and Benefits of Crime Prevention. *Crime and Justice 28*. Chicago, IL: Univ. of Chicago Press.

[N01b] Nagin, D. S. (2001b). Measuring Economic Benefits of Developmental Prevention Programs. Chapter 9 in Welsh, Farrington & Sherman. *Costs and Benefits of Preventing Crime*. Boulder, CO: Westview Press.

[NI05] novirdata Integration GmbH (P. Böhm) (2005). Big Spam-Business – Die Hintergründe der Spam- und Virus-Wirtschaft. Vortrag im Rahmen des 3rd German Anti-Spam Summit. Köln (Deutschland), 8. September 2005.

[NR04] Nucleus Research (o. V.) (2004). Spam: The Serial ROI Killer.

[P94] Portney, P. R. (1994). The Contingent Valuation Debate: Why Economists Should Care. *Journal of Economic Perspectives 8* (4), S. 3-17.

[Proj] Projektseite des ZEW-Branchenreport Dienstleister der Informationsgesellschaft (o. V.) (2009). PHP3-Datei online verfügbar unter `http://www.zew.de/de/publikationen/branchenreportdienstleistungen.php3` (Stand: 20.07.2009).

[SH90] Samples, K. C. und J. R. Hollyer (1990). Contingent Valuation of Wildlife Resources in the Presence of Substitutes and Complements. In R. Johnson und G. V. Johnson (Eds.). *Economic Valuation of Natural Resources: Issues, Theory and Applications*, S. 177-192. Boulder: Westview Press.

[SP93] Schkade, D. A. und J. W. Payne (1993). Where do the numbers come from? How people respond to Contingent Valuation Questions. In J. Hausman (Ed.). *Contingent Valuation: A Critical Assessment*, S. 271-304. Amsterdam: North Holland Press.

[SP94] Schkade, D. A. und J. W. Payne (1994). How People Respond to Contingent Valuation Questions: A Verbal Protocol Analysis of Willingness to Pay for an Environmental Regulation. *Environmental Economics and Management 26*, S. 88-109.

[SS05] Schleife, K. und O. Schmid (2005). IT-Sicherheit in Unternehmen. In I. Bertschek und T. Döbler (Hrsg.). *Open Source Software und IT-Sicherheit. FAZIT-Schriftenreihe, Forschungsbericht Bd. 1*, S. 81-97. Stuttgart.

[SU04] Schmeh, K. und H. Uebelacker (2004). Sicherheit, die sich rechnet – Return-on-Investment in der IT-Security. HTML-Datei online verfügbar unter `http://www.heise.de/tp/r4/artikel/18/18954/1.html` (Stand: 20.07.2009, Veröffentlichung: 06.12.2004).

[S05] Schoolmann, J. (2005). Kosten des IT-Sicherheitsprozesses. Rieger, H. & Schoolmann, J. (Hrsg.). *Praxishandbuch IT-Sicherheit*. Symposium Publishing GmbH.

[Sc04] Schryen, G. (2004). Effektivität von Lösungsansätzen zur Bekämpfung von Spam. *Wirtschaftsinformatik 46* (4), S. 281-288.

[SR+93] Schulze, W. D., R. D. Rowe, W. S. Breffle, R. Boyce und G. McClelland (1993). Contingent Valuation of Natural Resource Damages Due to Injuries to the Upper Clark Fork River Basin. (Report prepared for the State of Montana Natural Resource Damage Program).

[SWB04] Sipior, J. C., B. T. Ward und P. G. Bonner (2004). Should Spam be on the Menu? *Communications of the ACM 47* (6), S. 59-63.

[S07] Spamhaus (R. Cox) (2007). Good neighbours shun attractive nuisances. Vortrag im Rahmen des 5th German Anti-Spam Summit. Köln (Deutschland), 5. September 2007. PDF-Datei online verfügbar unter `http://www.eco.de/dokumente/6_Spamhaus-Fast-Flux_5dask2007.pdf` (Stand: 20.07.2009).

[Sp04] Spengler, H. (2004). Ursachen und Kosten der Kriminalität in Deutschland – drei empirische Untersuchungen. Dissertation, Technische Universität Darmstadt, Fachbereich Rechts- und Wirtschaftswissenschaften.

[SB08a] Statistisches Bundesamt Deutschland (o. V.) (2008). Binnenhandel, Gastgewerbe, Tourismus – Beschäftigte, Umsatz, Aufwendungen, Lagerbestände, Investitionen und Warensortiment im Handel. *Fachserie 6 Reihe 4 – 2006.*

[SB08b] Statistisches Bundesamt Deutschland (o. V.) (2008). Strukturerhebung im Dienstleistungsbereich – Verkehr und Nachrichtenübermittlung. *Fachserie 9 Reihe 1 – 2006.*

[SB08c] Statistisches Bundesamt Deutschland (o. V.) (2008). Strukturerhebung im Dienstleistungsbereich – Grundstücks- und Wohnungswesen, Vermietung beweglicher Sachen, Erbringung von wirtschaftlichen Dienstleistungen, a.n.g. . *Fachserie 9 Reihe 2 – 2006.*

[SB09] Statistische Ämter des Bundes und der Länder (o. V.) (2009). Erwerbstätige in den Ländern der Bundesrepublik Deutschland 1991 bis 2008 *Erwerbstätigenrechnung Reihe 1, Band 1.*

[StGB] Strafgesetzbuch (o. V.) (2009). PDF-Dokument online verfügbar unter `http://www.gesetze-im-internet.de/bundesrecht/stgb/gesamt.pdf` (Stand: 20.07.2009)

[TMG] Telemediengesetz (o. V.) (2009). PDF-Dokument online verfügbar unter `http://www.gesetze-im-internet.de/bundesrecht/tmg/gesamt.pdf` (Stand: 20.07.2009)

[V03] Vanberg, M. (2003). Die ZEW/Creditreform Konjunkturumfrage bei Dienstleistern der Informationsgesellschaft. ZEW Dokumentation Nr. 03-09. Mannheim.

[V05] Vanberg, M. (2005). *ZEW Branchenreport Dienstleister der Informationsgesellschaft Jahrgang 4*, Nr. 2. PDF-Datei online verfügbar unter `ftp://ftp.zew.de/pub/zew-docs/brep/archiv/2005_BraRepDL_IKT_2Q2005.pdf` (Stand: 20.07.2009)

[V06] Vanberg, M. (2006). *ZEW Branchenreport Dienstleister der Informationsgesellschaft Jahrgang 5*, Nr. 1. PDF-Datei online verfügbar unter `ftp://ftp.zew.de/pub/zew-docs/brep/archiv/2006_BraRepDL_IKT_1Q2006.pdf` (Stand: 20.07.2009)

[V04] Vircom (o. V.) (2004). Why Spammers Spam. PDF-Datei nach Anmeldung verfügbar unter `http://www.vircom.com`

[WJM92] Walsh, R. G., D. M. Johnson und J. R. McKean (1992). Benefits Transfer of Outdoor Recreation Demand Studies: 1968-1988. *Water Resources Research 28*, S. 707-713.

[W09] Wikipedia – Die freie Enzyklopädie / The Free Encyclopedia (2009) HTML-Dateien online verfügbar unter `http://de.wikipedia.org/wiki/Hauptseite` und `http://en.wikipedia.org/wiki/Main_Page` (Stand: 20.07.2009)

[ZCB00] Zarkin, G. A., S. C. Cates und M. V. Bala (2000). Estimating the Willingness to Pay for Drug Abuse Treatment: A Pilot Study. *Journal of Substance Abuse Treatment 18*, S. 149-159.

[Z02] ZDNet (Autor: R. Lemos) (2002). Security guru: Let's secure the Net. HTML-Datei online verfügbar unter `http://techupdate.zdnet.com/techupdate/stories/main/0,14179,5103462,00.html` (Stand: 20.07.2009, Veröffentlichung: 20.02.2002).

[Z05] Zhang, L. (2005). The CAN-Spam Act: An Insufficient Response to the Growing Spam Problem. *Berkeley Technology Law Journal 20*, S. 301-332.

Anhang A

Informationen zur ZEW Konjunkturumfrage

A.1 Aufschlüsselung der Branchen

Die Definition des IKT-Sektors der OECD dient als Grundlage für die Abgrenzung der befragten Unternehmen der ZEW-Konjunkturumfrage. Im Folgenden werden die in der Umfrage berücksichtigten Wirtschaftszweige mit der Klassifikation von 2003 und den Beschäftigtenzahlen aus dem Jahr der Umfrage nach Angaben des Statistischen Bundesamtes (Stand: 30. September 2006, veröffentlicht im Juli/Oktober 2008) aufgelistet. Insgesamt waren 2.223.925 Menchen in den beobachteten Branchen beschäftigt.

IKT-Dienstleister

Nr. des WZ	Wirtschaftszweig	Beschäftigte
	Software und IT-Dienste	419.100
72.10-72.60	Datenverarbeitung und Datenbanken	
71.33	Vermietung von Büromaschinen, Datenverarbeitungsgeräten und -einrichtungen	
	IKT-Handel	200.553
51.43.1, 51.43.3-3.4	Großhandel mit elektronischen Erzeugnissen und Zubehör	
51.84.0	Großhandel mit Büromaschinen und Software	
52.45.2	Einzelhandel mit Geräten der Unterhaltungselektronik und Zubehör	
52.49.5	Einzelhandel mit Computern, peripheren Einheiten und Software	
52.49.6	Einzelhandel mit Telekomunikationsendgeräten und Mobiltelefonen	
	Telekommunikationsdienstleister	203.750
64.3	Fernmeldedienste	

Wissensintensive Dienstleister

Nr. des WZ	Wirtschaftszweig	Beschäftigte
74.12.0-2.5	**Steuerberatung und Wirtschaftsprüfung**	313.969
	Unternehmensberatung	413.971
74.11	Rechtsberatung	
74.14.1-4.2	Unternehmensberatung	
74.13.1-3.2	Markt- und Meinungsforschung	
74.20.1-0.4	**Architekturbüros**	374.990[1]
74.20.5-0.9	**Technische Beratung und Planung**	
73.10.1-0.5, 73.20.1-0.2	Forschung und Entwicklung	93.892
74.40.1-0.2	**Werbung**	203.700

[1] Architektur- und Ing. -Büros sind in dieser Statistik zusammengefasst.

A.2 Liste der Variablennamen und Fragebogen

Variable	Erläuterung	Ausprägung
PCAnt	Anteil der Beschäftigten mit überwiegender Arbeit an einem PC, Laptop, Terminal oder Workstation	Prozent[2]
B2B	E-Commerce: selbst Bestellungen aufgeben	binär
B2C	E-Commerce: Bestellungen annehmen	binär
B2Cb	E-Commerce: Bestellungen von anderen Unternehmen annehmen	binär
B2Cc	E-Commerce: Bestellungen von Endkunden annehmen	binär
B2Cnein	KV[3]: keine Bestellungen von Anderen annehmen	binär
B2CAnt	Umsatzanteil mit E-Commerce 2005	Prozent[2]
B2CAntNein	KV[4]: kein Umsatz mit E-Commerce	binär
Ums2005	Umsatz[5] (in Tausend Euro) im Jahr 2005	ganzzahlig[6]
	Zahlungsbereitschaft Beobachtungsgruppe 1 und 4	
WTPMal30	Zahlungsbereitschaft für Malware -30%	ganzzahlig
WTPMal70	Zahlungsbereitschaft für Malware -70%	ganzzahlig
WTPSpam30	Zahlungsbereitschaft für Spam -30%	ganzzahlig
WTPSpam70	Zahlungsbereitschaft für Spam -70%	ganzzahlig
	Zahlungsbereitschaft Beobachtungsgruppe 2 und 3	
WTPMal50	Zahlungsbereitschaft für Malware -50%	ganzzahlig
WTPMal90	Zahlungsbereitschaft für Malware -90%	ganzzahlig
WTPSpam50	Zahlungsbereitschaft für Spam -50%	ganzzahlig
WTPSpam90	Zahlungsbereitschaft für Spam -90%	ganzzahlig
MalVorSpam	Kontrollvariable für Reihenfolge *(„Sequencing“)* 1 für Gruppe 1 und 2, 0 für Gruppe 3 und 4	binär
AnzMA	Anzahl der Mitarbeiter (MA) insgesamt[5]	ganzzahlig
AnzIT	Anzahl MA mit Ausbild. / Studium im IT-Bereich	ganzzahlig
AntIT	Anteil MA mit Ausbild. / Studium im IT-Bereich	Prozent[2]
AnzITnein	KV[4]: keine MA mit Ausbild. / Stud. im IT-Bereich	binär

[2]Die Werte liegen im Intervall $[0; 100]$ (Prozent).

[3]Die Variable war ursprünglich nur als Kontrollvariable zur Vermeidung von Missings gedacht, fand dann aber Eingang in die Analysen.

[4]Die Variable diente lediglich als Kontrollvariable zur Vermeidung von Missings.

[5]Die Angaben entstammen dem Fragebogen, nicht der Creditreform-Datenbank.

[6]Die Variable war im Datensatz zwar als Gleitkommazahl definiert, trotzdem waren alle verwendeten Werte ganzzahlig.

Variable	Erläuterung	Ausprägung
AnzAd	Anzahl MA (nur) für Administration	ganzzahlig
AntAd	Anteil MA (nur) für Administration	Prozent[2]
AnzAdnein	KV[4]: keine MA (nur) für Administration	binär
AnzITS	Anzahl MA (nur) für IT-Sicherheit	ganzzahlig
AntITS	Anteil MA (nur) für IT-Sicherheit	Prozent[2]
AnzITnein	KV[4]: keine MA (nur) für IT-Sicherheit	binär
AnzAdIT	Anzahl MA für Administration und IT-Sicherheit	ganzzahlig
AntAdIT	Anteil MA für Administration und IT-Sicherheit	Prozent[2]
AnzAdITnein	KV[4]: keine MA für Admin. und IT-Sicherheit	binär
SumAdITS	kumulierte Anzahl MA für Ad, ITS und AdIT	ganzzahlig
AntSumAI	kumulierter Anteil MA für Ad, ITS und AdIT	Prozent[2]
ITBerat	Beratung von externer Seite zur IT-Sicherheit	binär
ITBeratNein	keine Beratung von externer Seite zur IT-Sicherheit	binär
ITOutsrc	komplette Auslagerung der Administration („Outsourcing“)	binär
ITOutsrcTeil	teilweise Auslagerung der Administration	binär
ITOutsrcNein	keine Auslagerung der Administration	binär
WBAdm	Weiterbildung der Administratoren im Bereich IT-Sicherheit	binär
WBAnw	Weiterb. der Anwender im Bereich IT-Sicherheit	binär
AufkAnw	Aufklärung der Anwender über Gefahren aus dem Internet	binär
WBnein	keine Weiterbildung oder Aufklärung der MA	binär
AntSpam	geschätzter Anteil von Spam am Mail-Aufkommen	Prozent[2]
Mal2005	Vorfälle durch Malware im Jahr 2005	binär
Mal2004	Vorfälle durch Malware im Jahr 2004	binär
MalVor2004	Vorfälle durch Malware vor 2004	binär
MalNein	KV[3]: noch nie Vorfälle durch Malware	binär
AnzMalJahr	Anzahl der Jahre mit Vorfällen durch Malware	ganzzahlig
AntITS0105	Anteil für IT-Sicherheit am IT-Budget 1-5 %	binär
AntITS0610	Anteil für IT-Sicherheit am IT-Budget 6-10 %	binär
AntITS11plus	Anteil für IT-Sicherheit am IT-Budget >10 %	binär
AntITSkA	keine Angaben zum Anteil für IT-Sicherheit am IT-Budget	binär
AntITSmiss	Missing bei Anteil für IT-Sicherheit am IT-Budget	binär

Variable	Erläuterung	Ausprägung
B:EDV	Branche: EDV (Software und IT-Dienste)	binär
B:IKTHandel	Branche: IKT-Handel	binär
B:Telekomm	Branche: Telekommunikation	binär
B:Steuer	Branche: Steuerberatung und Wirtschaftsprüfung	binär
B:Untberat	Branche: Unternehmensberatung	binär
B:Architekt	Branche: Architekturbüros	binär
B:Techberat	Branche: Technische Beratung und Planung	binär
B:FundE	Branche: Forschung und Entwicklung	binär
B:Werbung	Branche: Werbung	binär
B:Miss	keine Angaben zur Branche	binär
RegWest	Region: Westdeutschland	binär
RegOst	Region: Ostdeutschland	binär

Fragebogen der Konjunkturumfrage

Bei dem auf der nächsten Seite (verkleinert) abgedruckten Fragebogen handelt es sich um Version 2 (siehe dazu auch Tabelle 4.1).

Bitte senden Sie den ausgefüllten Fragebogen bis **Freitag, den 17. März 2006, per Fax: Nr. 0621/1235-333 oder -225** (oder per Post, Gebühr zahlt Empfänger) zurück an das Zentrum für Europäische Wirtschaftsforschung (ZEW).

ZEW / CREDITREFORM Konjunkturumfrage

ZEW
Konjunkturumfrage
L 7, 1
68161 Mannheim

Beantworten Sie bitte die folgenden Fragen für Ihr Hauptgeschäftsfeld. Wir fragen Sie zuerst nach der Entwicklung **im laufenden Quartal (Januar bis März 2006)** gegenüber dem Vorquartal, dann nach der voraussichtlichen Entwicklung **im kommenden Quartal (April bis Juni 2006)**.

Ist der Umsatz Ihres Unternehmens...
❑ gestiegen ❑ gleich geblieben ❑ gesunken

Um wie viel Prozent ca.?
_____ Prozent ❑ keine Angabe

Wird der Umsatz Ihres Unternehmens...
❑ steigen ❑ gleich bleiben ❑ sinken

Um wie viel Prozent ca.?
_____ Prozent ❑ keine Angabe

Sind Ihre Preise...
❑ gestiegen ❑ gleich geblieben ❑ gesunken

Werden Ihre Preise...
❑ steigen ❑ gleich bleiben ❑ sinken

Hat sich Ihre Ertragslage...
❑ verbessert ❑ nicht verändert ❑ verschlechtert

Wird sich Ihre Ertragslage...
❑ verbessern ❑ nicht verändern ❑ verschlechtern

Ist die Nachfrage nach Ihren Dienstleistungen...
❑ gestiegen ❑ gleich geblieben ❑ gesunken

Wird die Nachfrage nach Ihren Dienstleistungen...
❑ steigen ❑ gleich bleiben ❑ sinken

Ist Ihr Personalbestand...
❑ gestiegen ❑ gleich geblieben ❑ gesunken

Wird Ihr Personalbestand...
❑ steigen ❑ gleich bleiben ❑ sinken

Wie hoch ist der Anteil der Beschäftigten in Ihrem Unternehmen, die den überwiegenden Teil der Arbeit an einem PC, Laptop, Terminal oder einer Workstation erledigen?
ca. _____ Prozent

Nutzen Sie in Ihren Geschäftsbeziehungen die Möglichkeit, Bestellungen über das Internet anzunehmen (E-Commerce)?
❑ Ja, von anderen Unternehmen ❑ Ja, von Endkunden ❑ Nein

Wie hoch war Ihr Umsatzanteil mit E-Commerce im Jahr 2005?
ca. _____ Prozent ❑ Nicht zutreffend

Nutzen Sie in Ihren Geschäftsbeziehungen zu anderen Unternehmen die Möglichkeit, Bestellungen über das Internet aufzugeben?
❑ Ja ❑ Nein

Wie hoch war der Umsatz Ihres Unternehmens im Jahr 2005?
ca. _____ Tausend Euro

Angenommen, Sie hätten keine Möglichkeit, sich selbst gegen Schadprogramme (Viren, Trojaner), Hacker und sonstige Gefahren aus dem Internet zu schützen. Wie viel wären Sie bereit pro Jahr an eine europäische Institution zu zahlen, die diese Gefahren aus dem Internet reduziert?
Reduzierung um 50% : _____ Euro um 90% : _____ Euro

Angenommen, Sie hätten keine Möglichkeit, einen eigenen Spamfilter einzurichten. Wie viel wären Sie bereit pro Jahr an eine europäische Institution zur Bekämpfung von Spam zu zahlen, um den Anteil der unerwünschten E-Mails (Spam) zu senken?
Senkung um 50% : _____ Euro um 90% : _____ Euro

Wie hoch ist die Anzahl Ihrer Mitarbeiter insgesamt?
_____ Mitarbeiter

Wie viele Ihrer Mitarbeiter haben eine Ausbildung oder ein Studium im IT-Bereich absolviert?
Anzahl Mitarbeiter: _____ ❑ keine

Wie viele Mitarbeiter sind bei Ihnen hauptsächlich für Systemadministration und die IT-Sicherheit beschäftigt?
Anzahl Mitarbeiter nur für Administration: _____ ❑ keine
Anzahl Mitarbeiter nur für IT-Sicherheit: _____ ❑ keine
Zusätzlich dazu für Administration und IT-Sicherheit: _____ ❑ keine

Werden Sie bei Fragen der IT-Sicherheit von externer Seite beraten?
❑ Ja ❑ Nein

Haben Sie die Administration Ihres IT-Bereichs an externe Unternehmen ausgelagert? („Outsourcing“)
❑ Ja, komplett ❑ Ja, teilweise ❑ Nein

Ermöglichen Sie Ihren Mitarbeitern die Weiterbildung im Bereich IT-Sicherheit bzw. klären Sie sie über mögliche Gefahren aus dem Internet auf? (Mehrfachnennung möglich)
❑ Weiterbildung der Administratoren
❑ Weiterbildung der Anwender
❑ Aufklärung der Anwender
❑ Keine Weiterbildung oder Aufklärung der Mitarbeiter

Wie hoch schätzen Sie den derzeitigen Anteil an Spam an Ihrem täglichen Mailaufkommen?
ca. _____ Prozent

Gab es in Ihrem Unternehmen bereits Vorfälle durch Schadprogramme (z.B. Viren, Trojaner)? (Mehrfachnennung möglich)
❑ Ja, in 2005 ❑ Ja, in 2004 ❑ Ja, vor 2004 ❑ Nein, noch nie

Wie groß war 2005 der Anteil für IT-Sicherheit am IT-Budget in Ihrem Unternehmen?
❑ 1 – 5 % ❑ 6 – 10 % ❑ › 10 % ❑ weiß nicht

Anhang B

Tabellen und Abbildungen zu Kapitel 5

Quantil	**Anz. MA**	**Umsatz 2005**	**Ums. pro MA**
Minimum	1	0	0,0
1%	1	2	0,1
5%	2	30	1,2
10%	4	149	25
25%	7	400	51
50%	20	1.217	80
75%	47	5.000	134
90%	140	20.000	285
95%	240	52.000	500
99%	2.500	800.000	5.208
Maximum	14.000	8.300.000	140.000
Anz. Beob.	782	662	638
Mittelwert	135	46.204	647
Std. Abw.	860	446.738	6.575

Erklärung: Umsatz sowie Umsatz pro Mitarbeiter in Tausend Euro (pro Mitarbeiter)

Tabelle B.1: Anzahl der Mitarbeiter und Umsatz im Jahr 2005

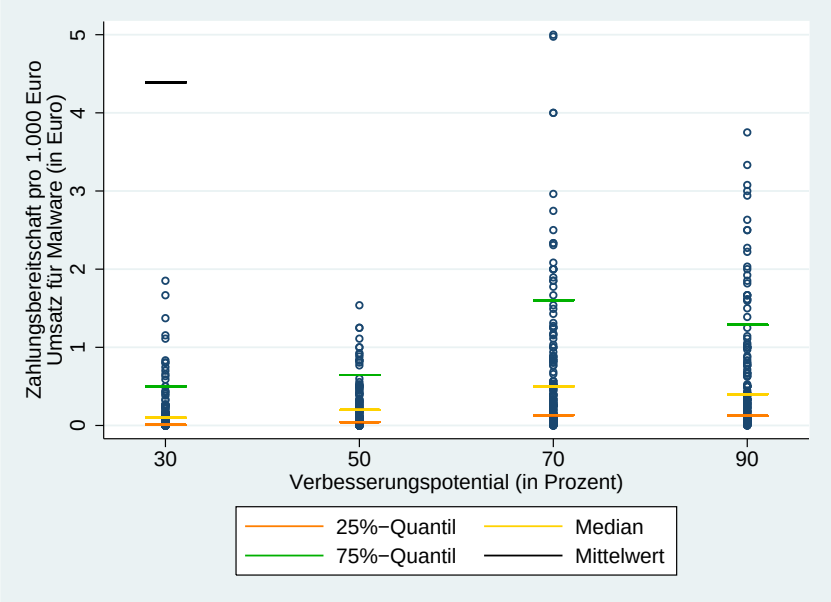


Abbildung B.1: Streuung WTP für Malware pro 1.000 Euro Umsatz

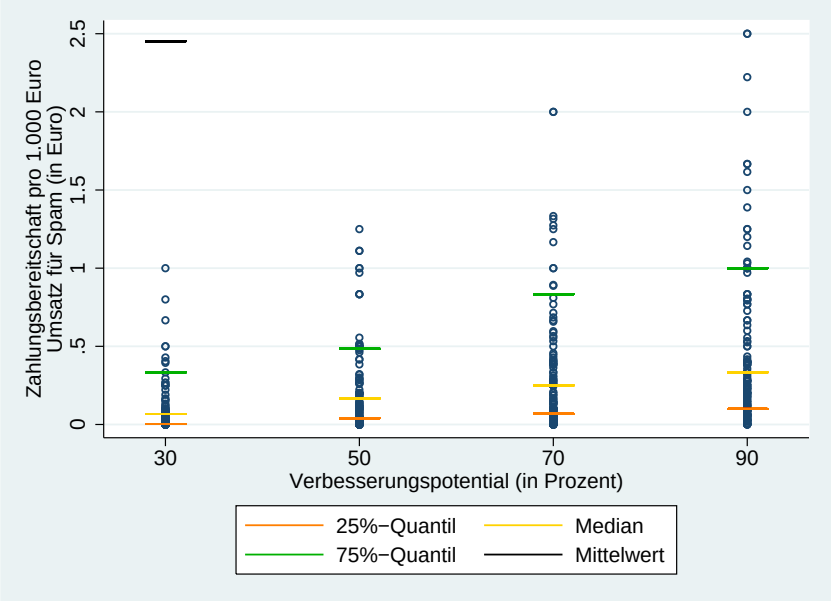


Abbildung B.2: Streuung WTP für Spam pro 1.000 Euro Umsatz

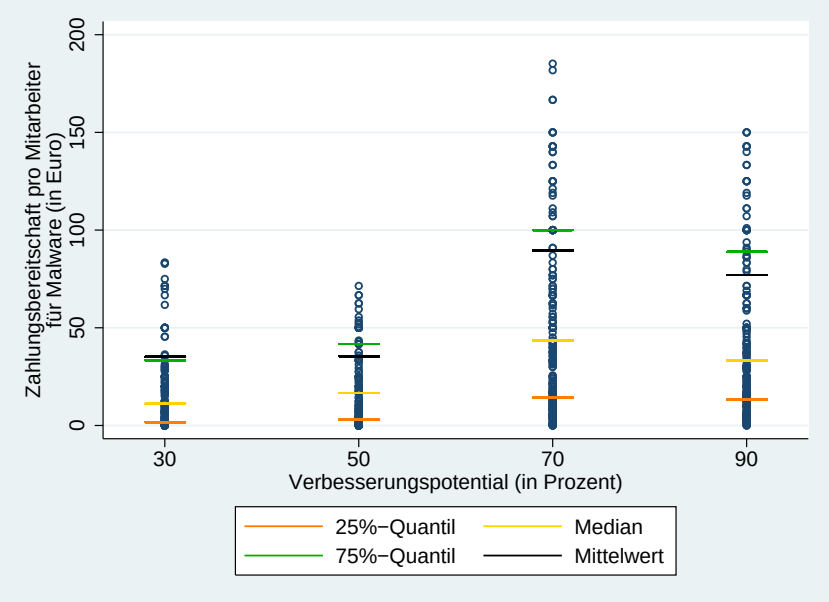


Abbildung B.3: Streuung WTP für Malware pro Mitarbeiter

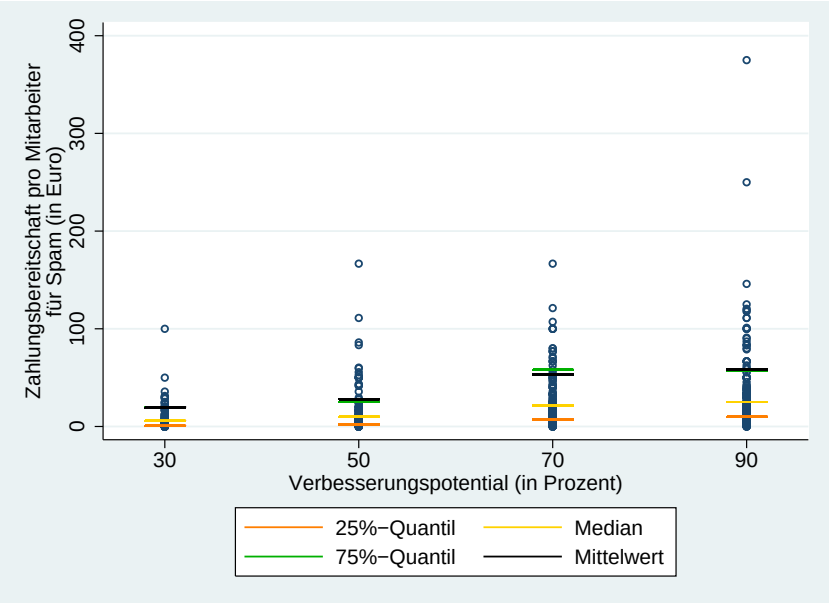


Abbildung B.4: Streuung WTP für Spam pro Mitarbeiter

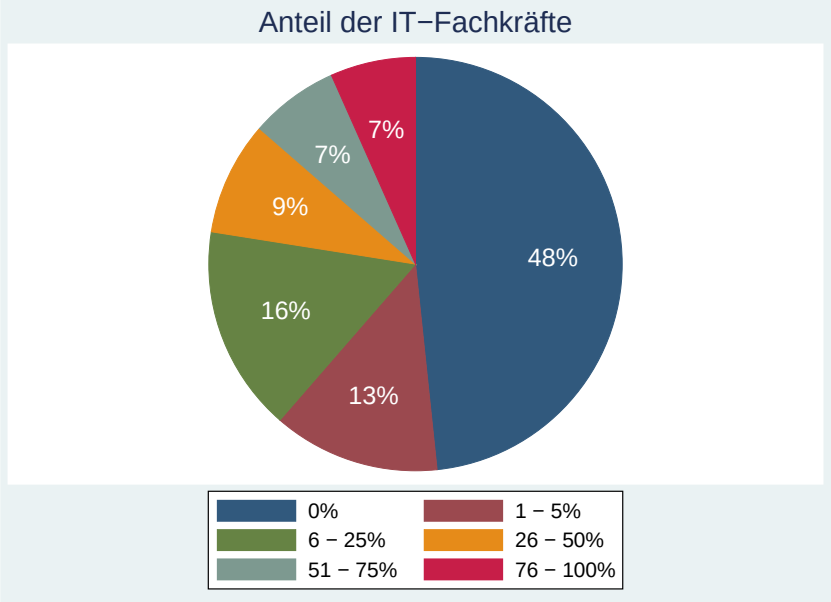


Abbildung B.5: Anteil der IT-Fachkräfte am Personal

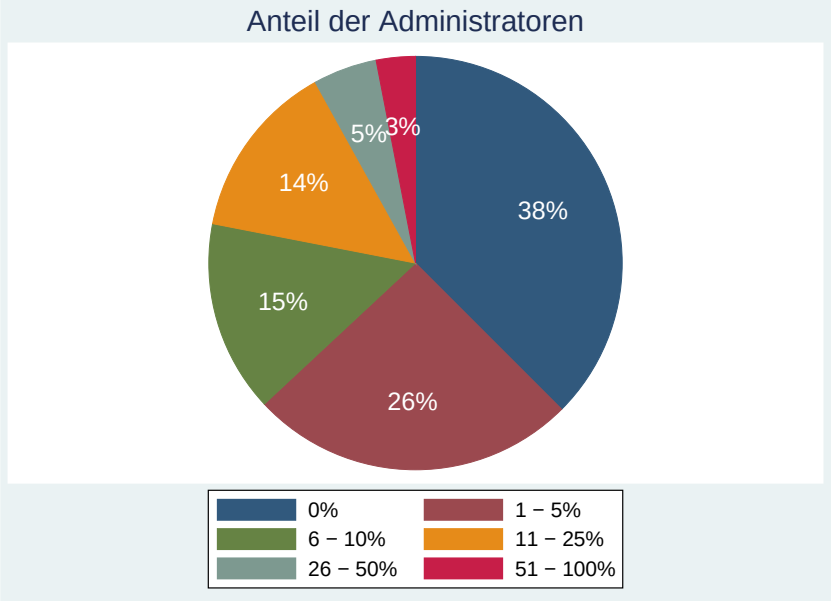


Abbildung B.6: Anteil der Mitarbeiter für Administration und IT-Sicherheit

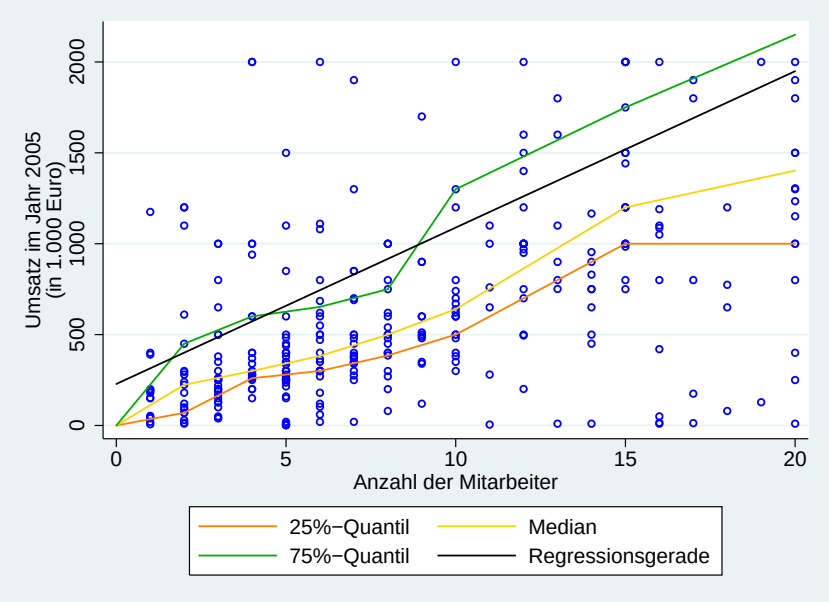


Abbildung B.7: Streuung von Umsatz und Personal bis 20 Mitarbeiter

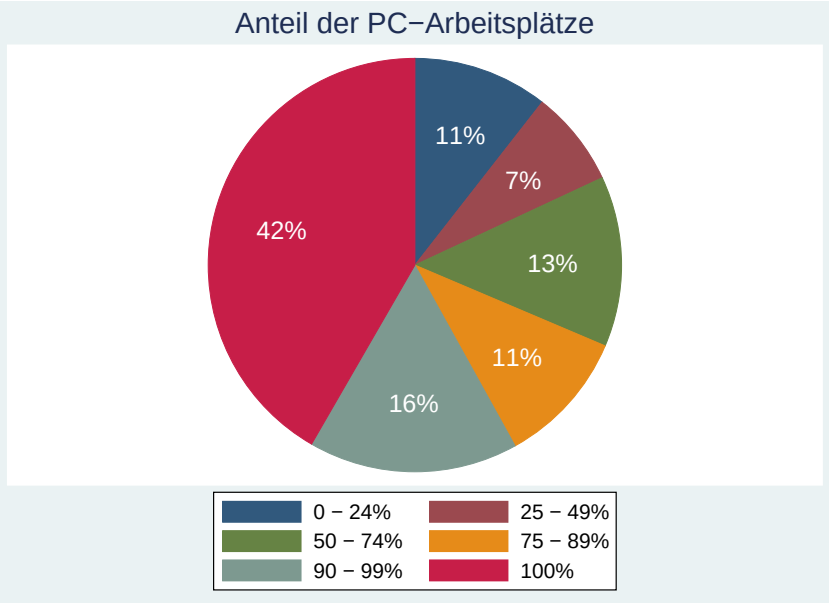


Abbildung B.8: Anteil der PC-Arbeitsplätze

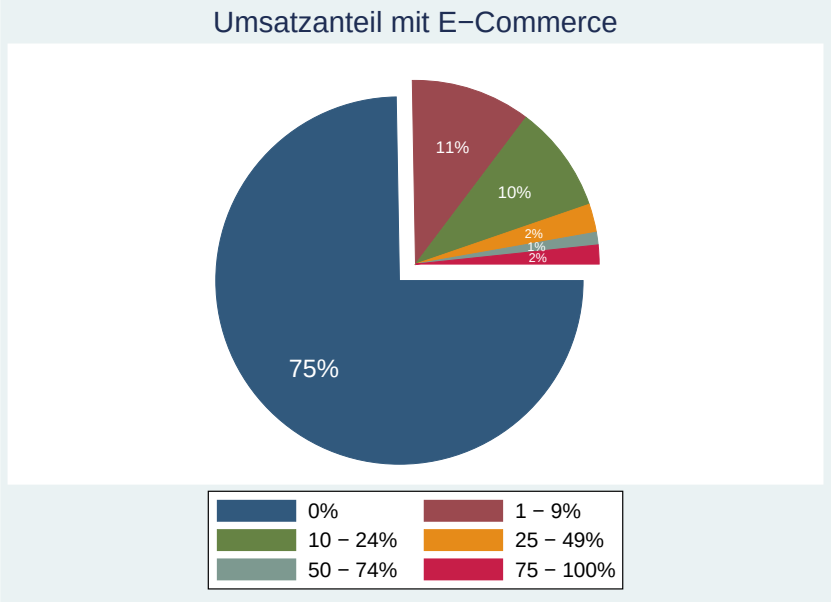


Abbildung B.9: Anteil des E-Commerce am Umsatz

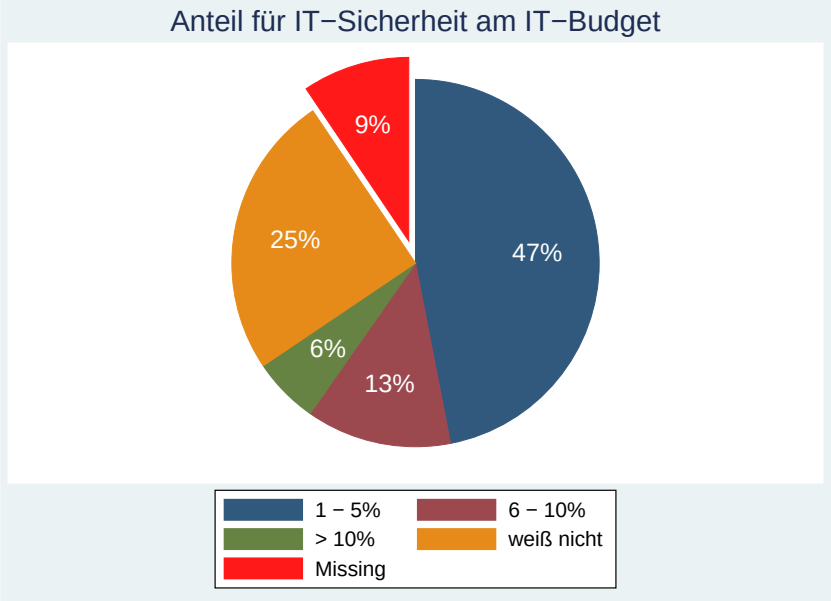


Abbildung B.10: Anteil für IT-Sicherheit am IT-Budget

WTP für Malware pro 1.000 Euro Umsatz												
	ohne Sequencing				an erster Stelle gefragt				an zweiter Stelle gefragt			
Quantil	30 %	50 %	70 %	90 %	30 %	50 %	70 %	90 %	30 %	50 %	70 %	90 %
Minimum	0	0	0	0	0	0	0	0,002	0	0	0	0,001
1%	0	0	0	0,002	0	0	0	0,003	0	0	0	0,001
5%	0	0	0,025	0,021	0	0	0,025	0,021	0	0	0,015	0,028
10%	0	0	0,056	0,050	0	0	0,045	0,050	0	0	0,056	0,056
25%	0,009	0,043	0,150	0,130	0,008	0,045	0,205	0,167	0,028	0,043	0,132	0,100
50%	0,115	0,200	0,505	0,400	0,100	0,185	0,769	0,400	0,133	0,265	0,455	0,431
75%	0,500	0,645	1,775	1,500	0,610	0,570	2,703	1,290	0,500	0,805	1,250	1,818
90%	2,232	1,942	5,000	4,286	2,882	2,429	10,00	3,333	1,373	1,316	2,746	5,000
95%	5,000	10,00	12,50	20,00	5,000	15,00	12,50	17,39	3,676	3,356	6,667	20,00
99%	200,0	333,3	400,0	600,0	200,0	333,3	500,0	234,4	111,1	1000,0	222,2	2000,0
Maximum	200,0	1000,0	500,0	2000,0	200,0	333,3	500,0	600,0	111,1	1000,0	222,2	2000,0
Anz. Beob.	131	142	182	189	60	80	83	103	71	62	99	86
Mittelwert	4,578	13,68	10,91	20,23	7,276	10,09	18,76	11,00	2,299	18,34	4,325	31,28
Std. Abw.	26,34	92,07	58,31	156,7	36,11	50,77	82,04	64,66	13,35	127,3	23,51	221,5

Tabelle B.2: Zahlungsbereitschaft für Malware pro 1.000 Euro Umsatz

WTP für Spam pro 1.000 Euro Umsatz												
	ohne Sequencing				an erster Stelle gefragt				an zweiter Stelle gefragt			
Quantil	30 %	50 %	70 %	90 %	30 %	50 %	70 %	90 %	30 %	50 %	70 %	90 %
Minimum	0	0	0	0,001	0	0	0	0,001	0	0	0	0,001
1%	0	0	0	0,001	0	0	0	0,001	0	0	0	0,001
5%	0	0	0,013	0,021	0	0	0,013	0,029	0	0	0,007	0,007
10%	0	0	0,028	0,038	0	0,001	0,039	0,038	0	0	0,250	0,038
25%	0,008	0,04	0,091	0,125	0,009	0,040	0,091	0,100	0,004	0,040	0,100	0,143
50%	0,077	0,167	0,282	0,333	0,066	0,167	0,250	0,333	0,087	0,167	0,400	0,345
75%	0,333	0,500	0,893	1,000	0,405	0,500	0,833	1,000	0,293	0,485	1,250	1,042
90%	0,909	1,250	2,882	2,727	0,667	1,111	1,948	2,500	1,429	1,250	5,000	3,077
95%	2,000	8,696	8,000	10,00	1,053	3,704	4,464	5,556	5,000	8,696	10,00	12,86
99%	8,000	300,0	100,0	600,0	8,000	500,0	30,00	1000,0	100,0	300,0	200,0	600,0
Maximum	100,0	500,0	200,0	1000,0	8,000	500,0	30,00	1000,0	100,0	300,0	200,0	600,0
Anz. Beob.	127	138	170	181	71	63	95	83	56	75	75	98
Mittelwert	1,182	7,160	2,975	10,26	0,389	10,04	1,175	13,47	2,188	4,745	5,254	7,552
Std. Abw.	8,902	50,07	17,29	86,41	1,132	63,98	3,757	109,7	13,34	34,61	25,60	60,56

Tabelle B.3: Zahlungsbereitschaft für Spam pro 1.000 Euro Umsatz

Tabelle B.4: Zahlungsbereitschaft für Malware pro Mitarbeiter

WTP für Malware pro Mitarbeiter												
	ohne Sequencing				an erster Stelle gefragt				an zweiter Stelle gefragt			
Quantil	30 %	50 %	70 %	90 %	30 %	50 %	70 %	90 %	30 %	50 %	70 %	90 %
Minimum	0	0	0,056	0,090	0	0	1,515	0,090	0	0	0,056	1,250
1%	0	0	0,833	1,250	0	0	1,515	0,526	0	0	0,667	1,250
5%	0	0	4,000	2,500	0	0	5,000	2,500	0	0	2,857	3,472
10%	0	0	6,000	4,000	0	0	10,00	3,571	0	0	5,263	5,000
25%	2,500	3,030	15,50	13,48	2,083	3,750	21,43	14,29	2,500	2,500	12,50	10,77
50%	12,50	16,67	50,00	33,33	14.14	14,29	66,67	36,11	9,630	16,67	33,33	33,33
75%	34,52	37,50	103,6	92,33	50,00	50,00	133,3	92,33	29,29	33,33	76,92	91,67
90%	90,91	80,00	200,0	163,9	100,0	95,24	227,3	200,0	83,05	52,63	166,7	142,9
95%	142,9	100,0	333,3	250,0	150,0	120,0	400,0	400,0	133,9	66,67	272,7	166,7
99%	300,0	588,2	769,2	666,7	250,0	857,1	769,2	882,4	694,4	117,6	1000,0	635,7
Maximum	694,4	857,1	1041,7	1714,3	250,0	857,1	769,2	1714,3	694,4	117,6	1041,7	635,7
Anz. Beob.	148	155	204	208	68	89	93	116	80	66	111	92
Mittelwert	36,06	35,16	92,54	79,32	35,36	44,41	107,0	94,70	36,66	22,68	80,40	59,93
Std. Abw.	73,99	87,24	145,9	158,5	50,69	112,6	134,5	198,4	89,50	24,50	154,3	81,92

WTP für Spam pro Mitarbeiter												
	ohne Sequencing				an erster Stelle gefragt				an zweiter Stelle gefragt			
Quantil	30 %	50 %	70 %	90 %	30 %	50 %	70 %	90 %	30 %	50 %	70 %	90 %
Minimum	0	0	0,125	0,045	0	0	0,125	0,333	0	0	1,176	0,045
1%	0	0	0,222	0,333	0	0	0,222	0,333	0	0	1,176	0,500
5%	0	0	1,818	2,083	0	0	1,818	1,667	0	0	2,247	2,143
10%	0	0	4,032	2,857	0	0	3,846	3,636	0	0	5,000	2,679
25%	1,429	2,500	8,333	10,00	1,600	2,024	7,143	10,00	1,062	4,167	17,50	11,11
50%	6,875	10,71	25,00	28,57	5,000	9,259	16,67	25,00	9,545	12,77	33,33	30,00
75%	20,00	25,00	66,67	58,82	23,08	20,00	55,32	50,00	20,00	33,33	76,92	66,67
90%	50,00	58,82	142,9	133,3	50,00	42,86	107,1	100,0	61,73	83,33	166,7	155,0
95%	100,0	100,0	200,0	222,2	100,0	58,82	150,0	133,3	83,33	111,1	233,3	250,0
99%	250,0	250,0	500,0	666,7	250,0	250,0	500,0	375,0	250,0	857,1	769,2	666,7
Maximum	250,0	857,1	769,2	1714,3	250,0	250,0	500,0	375,0	250,0	857,1	769,2	1714,3
Anz. Beob.	142	151	189	199	78	69	104	89	64	82	85	110
Mittelwert	20,23	28,37	58,14	60,76	19,16	18,95	47,26	40,42	21,52	36,30	71,45	77,22
Std. Abw.	37,43	76,55	99,30	141,9	37,02	36,86	85,97	52,27	38,17	97,83	112,6	183,7

Tabelle B.5: Zahlungsbereitschaft für Spam pro Mitarbeiter

Anhang C

Auszug aus der Polizeilichen Kriminalstatistik (PKS)

Berichtsjahre 1998-2007 der Polizeilichen Kriminalstatistik

veröffentlicht 1999-2008 [PKS99] - [PKS08]

Die Tabelle enthält die erfassten Fälle, bei ausgewählten Deliktsarten sind die Aufklärungsquoten in Klammern angegeben.

Tabelle C.1: Auszug aus der PKS: Computerkriminalität

Schlüssel	Straftaten(gruppen)	2007	2006	2005	2004	2003	2002	2001	2000	1999	1998
8970	Computerkriminalität	62.944	59.149	62.186	66.973	59.691	57.488	79.286	56.699	45.369	46.076
	davon:										
5163	Betrug mittels rechtswidrig erlangter Debitkarten mit PIN	25.348	27.347	32.232	36.088	35.954	36.969	48.610	44.284	36.613	35.909
5175	Computerbetrug -§ 263 a StGB-	16.274 (37,2)	16.211 (48,9)	15.875 (48,7)	14.186 (46,4)	11.388 (43,2)	9.531 (57,0)	17.310 (77,9)	6.600 (67,0)	4.474 (54,9)	6.465 (60,7)
5179	Betrug mit Zahlungsberechtigungen zu Kommunikationsdiensten	5.998 (60,7)	5.822 (57,7)	5.788 (64,4)	7.357 (66,2)	7.003 (67,0)	5.902 (77,1)	8.039 (84,2)	2.198 (81,5)	1.412 (88,1)	2.109 (31,5)
5430	Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei Datenverarbeitung -§§ 269, 270 StGB-	4.419	2.460	1.012	570	237	228	920	268	124	349
6742	Datenveränderung, Computersabotage -§§ 303 a, 303 b StGB-	2.660 (24,3)	1.672 (29,0)	1.609 (35,9)	3.130 (44,2)	1.705 (39,3)	1.327 (38,1)	862 (45,4)	513 (52,6)	302 (57,6)	326 (40,2)
6780	Ausspähen von Daten	4.829 (32,8)	2.990 (43,8)	2.366 (42,2)	1.743 (38,0)	781 (57,6)	806 (64,4)	1.463 (82,6)	538 (46,1)	210 (65,2)	267 (80,1)
7151	Softwarepiraterie (private Anwendung z.B. Computerspiele)	2.979	1.920	2.667	2.782	2.053	1.947	1.672	1.361	972	362
7152	Softwarepiraterie in Form gewerbsmäßigen Handelns	437	727	637	1.117	570	780	410	937	1.252	289

Anhang D

Glossar

Anti-Viren-Programm: auch Anti-Viren-Software oder Viren-Schutz; → Software, die als Schutzmaßnahme bekannte → Malware sucht, entdeckt und (wenn gewünscht) entfernen kann.

Backdoor: zu Deutsch „Hintertür"; oft Bestandteil der Schadroutine moderner → Malware; ermöglicht unbefugten Zugriff auf befallenen Rechner durch Umgehung der Zugangssicherungsmechanismen.

Bandbreite: verfügbares Übertragungsvolumen aus der Datenübertragungstechnik.

Blacklists: auch Schwarze Listen oder Negativlisten genannt; enthalten im Bezug auf → Spam-Filterung Absender-Adressen, → -Domänen oder → -IPs, von denen häufig Spam-Mails verschickt werden, so dass im Zuge der Filterung verdächtige Mails gekennzeichnet oder gelöscht werden können. Solche Listen können lokal gepflegt werden, sie werden aber auch im → Internet von verschiedenen Anbietern zur Verfügung gestellt. *Blacklists* sind erheblich weniger restriktiv als → *Whitelists,* da bei Negativlisten nur die E-Mails abgelehnt (oder gekennzeichnet) werden, die als von bekannten Spammern verschickt klassifiziert wurden, alle anderen Nachrichten werden akzeptiert.

Botnetz: Netzwerk von kompromittierten Rechnern, die ferngesteuert werden („Bots"). Eine ausführliche Erklärung erfolgt auf Seite 17.

CERT: ***C**omputer **E**mergency **R**esponse **T**eam,* zu Deutsch „Computer-Notfall-Team“; befasst sich mit → IT-Sicherheit, veröffentlicht als informierende und beratende Instanz Warnungen und leitet bei konkreten Vorfällen Gegenmaßnahmen ein und koordiniert sie.

Chatroom: vom englischen *„chat“* (Unterhaltung, Plauderei) und Raum; ein virtueller Raum, in dem mehrere Benutzer in Echtzeit kommunizieren können.

Contentfilter: zu Deutsch Inhaltsfilter; untersuchen E-Mails auf bestimmte Begriffe oder Wortgruppen, um auf diese Weise ihren Inhalt nach den Vorgaben des Empfängers auf Erwünschtheit bzw. Unerwünschtheit zu überprüfen, so lassen sich Begriffe als unerwünscht einstufen, andere als erwünscht kategorisieren.

Cybercrime: zu Deutsch Computerkriminalität; die Aufschlüsselung erfolgt in Anhang C.

Cyberspace: virtueller Raum, häufig synonym verwendet für das → Internet.

(D)DoS: ***(D**istributed) **D**enial **o**f **S**ervice;* siehe → *Denial of Service.*

Denial of Service: zu Deutsch „Dienstverweigerung“; Angriff auf Rechner, zumeist → Server, um von ihm zur Verfügung gestellten Dienst unerreichbar zu machen; erfolgt üblicherweise durch Überlastung des Zielcomputers, häufig sind Web-Server Opfer, um von ihnen angebotene Webseiten unzugänglich zu machen. Da angegriffene Server meistens für sehr große Zahl von Anfragen ausgelegt sind, erfolgen Angriffe gebündelt von einer großen Anzahl von Rechnern aus, diese Attacken werden als *Distributed Denial of Servive* bezeichnet *(DDoS).* Angriffe werden hauptsächlich auf zwei Arten durchgeführt, als (Teil der) Schadroutine von → Malware oder über → Botnetze; durch erfolgreiche (D)DoS-Attacke wird die → Verfügbarkeit des angegriffenen Systems eingeschränkt.

Domäne: ein (zusammenhängender) Adressbereich im → Internet wie beispielsweise `tu-darmstadt.de` .

E-Commerce: zu Deutsch „elektronischer Handel“; die Verlagerung oder Ausweitung des Handelsverkehrs auf das → Internet.

Embedding: auch *Nesting* genannt; kann auftreten, wenn im Rahmen einer CVM-Befragung ein zu bewertendes Gut vom Probanden in ein anderes Gut „eingebettet“ wird und dadurch die geäußerten Zahlungsbereitschaften nur geringfügig zwischen den Gütern differiert. Eine ausführliche Erklärung erfolgt ab Seite 59.

Filesharing: vom englischen *„share“* ((ver)teilen, teilhaben) und Datei, zu Deutsch „gemeinsamer Dateizugriff“; → *Peer-to-Peer*-Netzwerke wie Internet-Tauschbörsen *„Morpheus“* oder *„KaZaA“* dienen zur (illegalen) Vervielfältigung von Musik-Dateien, Filmen sowie Computerprogrammen und -spielen. → Würmer nutzen Infrastruktur zur Verbreitung durch Tarnung unter vielversprechenden, weil gefragten Dateinamen; werden von ahnungslosen Opfern auf PC geladen und dort von ihnen selbst gestartet.

Hardware: Sammelbegriff für Computer-Komponenten und Peripherie-Geräte; Gegenstück zur → Software.

Harvester: zu Deutsch „Erntemaschine“; E-Mail-→ Würmer, die sich nicht nur der Adressbücher infizierter Rechner bedienen, sondern die Rechner regelrecht nach Adressen durchsuchen, beispielsweise in → HTML-Dateien oder Word-Dokumenten.

Helpdesk: Informationsdienst zur Beratung und Unterstützung von Anwendern oder Kunden.

Hoax: vom englischen Wort für „Jux“, „Scherz“, „Schabernack“; Falschmeldung, beispielsweise per E-Mail verschickt; in einigen wird vor angeblichen → Malware-Bedrohungen gewarnt, haben oft aber nur den Charakter von (elektronischen) Kettenbriefen; richten üblicherweise keine tatsächlichen Schäden an, verursachen aber Kosten durch Erhöhung des E-Mail-Aufkommens und Arbeitszeitverluste, sowohl bei Empfängern als auch bei zurate gezogenen Administratoren.

HTML-Code: ***Hyper**text **M**arkup **L**anguage,* zu Deutsch „Hypertext-Auszeichnungssprache“; dient der Strukturierung von Texten, Bildern und → *Links* in HTML-Dateien zur Darstellung in Webbrowsern.

Inhaltsfilter: siehe → *Contentfilter.*

Integrität: ist gegeben, wenn Daten vollständig und unverändert sind und nur von Befugten modifiziert werden können. Die Integrität kann durch die Festlegung von Zugriffsrechten gewährleistet werden, um eine unerlaubte Veränderung zu verhindern, sie ist aber auch gegeben, wenn alle Veränderungen nachvollziehbar sind.

Internet: englisches Kofferwort, zusammengesetzt aus *„interconnected“* für „untereinander verbunden“ und *„networks“* für Netzwerke; weltweites Netzwerk aus vielen Rechnernetzen zum Austausch von Daten.

IP: ***I**nternet **P**rotocol;* eine IP bzw. IP-Adresse wie z. B. `130.83.201.1` wird zur Adressierung von Computern sowie von anderen netzwerkfähigen Geräten im → Internet verwendet.

IT-Sicherheit: gemäß Leitfaden für IT-Sicherheit (2007) des Bundesamtes für Sicherheit in der Informationstechnik (BSI) werden → Vertraulichkeit, → Verfügbarkeit und → Integrität als die drei Grundwerte der IT-Sicherheit angesehen. Außerdem sind gemäß Schleife und Schmid (2005, S. 85 f) noch die Authentizität sowie die Verbindlichkeit wichtig.

Kohärenz: erwünschte Eigenschaft von Risikomaßen, wenn sie positiv homogen, monoton, translationsinvariant und subadditiv ($f(x + y) \leq f(x) + f(y)$) sind.

Konfidenzintervall: gibt die Fehlerwahrscheinlichkeit bei der Schätzung von Parametern an.

Korrelation: linearer Zusammenhang zwischen mehreren statistischen Variablen, ohne Aussage über die Existenz kausaler Zusammenhänge zwischen zwei Variablen oder über eine dritte.

Kriminometrie: empirische Kriminalitätsforschung, ein interdisziplinäres Forschungsgebiet zur Erforschung von Ursachen oder ökonomischen Auswirkungen von Kriminalität.

Likert-Skala: Ordinales Skalierungsverfahren zur Messung persönlicher Einstellungen mittels sogenannter Items; auf 3-Punkte-Likert-Skala wären auf eine Frage z. B. „stimme zu“, „neutral“ und „stimme nicht zu“ mögliche Antworten.

Link: eigentlich Hyperlink, zu Deutsch Verknüpfung oder Verweis; verweist auf andere Quellen im → *World Wide Web.*

Malware: zu Deutsch Schadprogramm(e); Oberbegriff für → Viren, → Würmer und →„Trojaner“. Eine ausführliche Erklärung erfolgt ab Seite 11.

Newsgroup: Nachrichten- und Diskussionsforen im → Internet.

Normalverteilung: auch Gauß-Verteilung oder Gauß-Glocke genannt; Wahrscheinlichkeitsverteilung.

Open Source Software: ist „quelloffen“, d. h. der Quelltext ist frei verfügbar und der Einsatz der → Software kostenlos, daher ist die Verbreitung und die Nutzung der Software erlaubt.

Opportunitätskosten: Entgangene Erlöse, die durch Wahl einer anderer Alternative nicht realisiert werden können; keine eigentlichen Kosten.

Outsourcing: zu Deutsch Auslagerung; Fremdvergabe von Unternehmensaufgaben an Drittunternehmen.

Peer-to-Peer: vom englischen *„peer“* (Gleichgestellter, gleichrangig); direkte Verbindung(en) zwischen gleichberechtigten Rechnern innerhalb eines Netzwerks.

Personal Firewall: zu Deutsch „Persönliche Brand(schutz)mauer“, auch Desktop Firewall; → Software, die als Schutzmaßnahme Datenverkehr zwischen Rechner und Netzwerk filtert.

Perzentil: Lagemaß, unterteilt statistische Verteilung in 100 → Quantile.

Phishing: vom englischen Wort *„fishing“* für „angeln“ oder „fischen“ abgeleitet, beschreibt bildlich das „Angeln nach Passwörtern“; Schreibweise geht vermutlich auf → *Phreaking* zurück. Computerbetrug nach § 263 a StGB, dabei werden gefälschte E-Mails verschickt, welche den Anschein erwecken sollen, von Banken mit Onlinebanking oder Bezahlsystemen wie Paypal zu stammen, auch → Internet-Auktionshäuser und andere Webseiten, bei denen es für Täter lukrativ sein kann, Zugangsdaten wie Passwörter zu ergattern, sind im Visier der Betrüger. In E-Mails von Banken werden Kunden – aber auch Nichtkunden – aufgefordert werden, Kontodaten sowie PINs und TANs auf einer angeblich von der Bank stammenden Webseite anzugeben; geschieht unter dem Vorwand, Kundendatenbank zu aktualisieren oder aus Sicherheitsgründen eine noch verfügbare PIN/TAN-Kombination abzufragen; Täter können sich so Zugang zu Bankkonten verschaffen und haben dazu (mindestens) eine Überweisung zur freien Verfügung.

Phreaking: englisches Kofferwort, zusammengesetzt aus *„phone“* für Telefon und *„freak“* für Begeisterter; üblicherweise (illegales) Manipulieren von Telefonen und damit verbundene kostenlose Nutzung.

Portfolio: vom lateinischen *„portare“* (tragen) und *„folium“* (Blatt); Sammlung von Objekten gleichen Typs, z. B. Aktien.

Provider: vom lateinischen *„providere“* (versorgen); Dienstleister, z. B. Anbieter von Internet-Diensten wie E-Mail-Service.

Quantil: Lagemaß, unterteilt statistische Verteilung in gleich große Abschnitte; typische Quantile sind Median, Quartile und → Perzentile.

Reaktanz: in der Sozialpsychologie Widerstand gegen Bedrohungen der Freiheit wie beispielsweise Nötigung oder Zwang, Abwehrreaktion gegen Beschränkungen wie Verbote oder Zensur.

Schadprogramm: siehe → Malware.

Schwarze Listen: siehe → *Blacklists.*

Sequencing: kann auftreten, wenn im Rahmen einer CVM-Befragung mehrere Zahlungsbereitschaften geäußert werden sollen und die Reihenfolge Einfluss auf die Höhe der geäußerten Zahlungsbereitschaften hat. Eine ausführliche Erklärung erfolgt ab Seite 62.

Server: zu Deutsch „Diener"; (→ Hardware:) Computer (auch Host genannt), auf dem Server-Programme laufen; (→ Software:) Programm, das anderen Computern Dienstleistungen zur Verfügung stellen.

SMTP-Engine: ***S****imple* ***M****ail* ***T****ransfer* ***P****rotocol,* zu Deutsch „Einfaches E-Mail-Transport-Protokoll"; dient zur Übertragung von E-Mails in Computer-Netzwerken. Eine eigene SMTP-Engine ermöglicht → Malware Versand von E-Mails unabhängig von auf dem infizierten Rechner verfügbaren Programmen.

Software: Sammelbegriff für ausführbare Programme und Daten; Gegenstück zur → Hardware.

Spam: unerwünschte E-Mails, deren genaue Definition schwierig ist. Eine ausführliche Erklärung erfolgt ab Seite 18.

Trojaner: → Malware-Typ in Anlehnung an griechische Mythologie, eigentlich „Trojanisches Pferd" (englisch: „trojan horse"); ist selbst nicht in der Lage, sich zu replizieren, ist zur Verbreitung auf andere Schadprogramme angewiesen; enthält neben angepriesenem Nutzen ungewollte weitere Inhalte; die Eigenschaft, nützliche mit vom Benutzer verborgenen Funktionen zu verbinden, wird häufig als grundlegende Definition angesehen. Trojanische Pferde werden im allgemeinen Sprachgebrauch häufig als Trojaner (englisch: „trojan(s)") bezeichnet, die Kurzform ist zwar historisch nicht korrekt, da die Trojaner Opfer der Kriegslist waren, dennoch kann der Begriff ohne Missverständnisse verwendet werden.

Verfügbarkeit: liegt vor, wenn ein autorisierter Benutzer zum gewünschten Zeitpunkt auf Dienstleistungen und Funktionen eines IT-Systems zugreifen kann, dazu gehören u. A. Daten oder Programme. Die Verfügbarkeit kann beeinträchtigt werden, wenn durch gezielte Angriffe

Informationen oder Dienste nicht mehr oder nur eingeschränkt zur Verfügung stehen, beispielsweise durch eine Systemüberlastung, welche durch eine → *Denial of Service*-Attacke hervorgerufen wurde.

Vertraulichkeit: muss gewährleistet werden, indem unbefugter Zugriff beispielsweise durch Verschlüsselung der Daten verhindert wird, dies gilt sowohl für gespeicherte Daten, als auch für den Datentransfer zwischen zwei zugangsberechtigten Partnern. Die Vertraulichkeit ist nicht mehr gegeben, wenn Daten oder der Schlüssel zu ihnen in die Hände Dritter fällt, beispielsweise wenn eine nicht autorisierte Person sich durch Vortäuschung der Identität eines Zugangsberechtigten Zugriff auf die geschützten Informationen verschafft.

Virus: → Malware-Typ in Anlehnung an den Virus (Latein u. A. für „Gift“) aus Biologie und Medizin; befällt Dateien oder Datenträger, infiziert sie meistens nur einmal, kann lange unentdeckt bleiben und in manchen Fällen mutieren; ist auf einen Wirt angewiesen, unterscheidet sich dadurch von anderen Malware-Typen, verbreitet sich über Verbreitung der infizierten Datei(en) bzw. Datenträger.

Weiße Listen: siehe → *Whitelists.*

Whitelists: auch Weiße Listen oder Positivlisten genannt; enthalten im Bezug auf → Spam-Filterung Informationen über die Absender, die als vertrauenswürdig bzw. als erwünscht eingestuft wurden und deren Nachrichten deshalb immer zugestellt werden sollen. *Whitelists* sind erheblich restriktiver als die → *Blacklists,* da bei Positivlisten nur die E-Mails eines eingetragenen kleinen Kreises von Personen und Institutionen zugelassen werden.

World Wide Web: kurz WWW, zu Deutsch Weltweites Netz; Hypertext-System (siehe → HTML) im → Internet.

Wurm: → Malware-Typ in Anlehnung an die Lebewesen aus der Biologie (englisch: „worm(s)“); eigenständiges, selbst lebensfähiges Programm; verbreitet sich selbstständig u. A. per E-Mail, → *Peer-to-Peer*-Verbindungen wie Internet-Tauschbörsen *(→ Filesharing),* Netzlaufwerke und -freigaben oder Sicherheitslücken.

Kurzbiographie

Nach Erlangung der Allgemeinen Hochschulreife und Ableistung des Grundwehrdienstes hat Oliver Schmid von 1994 bis 2002 an der Universität Mannheim den Diplomstudiengang Wirtschaftsinformatik absolviert. Ab 1996 arbeitete er als Wissenschaftliche Hilfskraft an der Fakultät für Mathematik und Informatik. Von 2002 bis 2008 war er Wissenschaftlicher Mitarbeiter am Fachgebiet für Empirische Wirtschaftsforschung und Mikroökonometrie im Institut für Volkswirtschaftslehre der Technischen Universität Darmstadt, wo er ab 2004 auch Doktorand war. Seit 2009 arbeitet er als Wissenschaftlicher Mitarbeiter an der Universität Trier am Kompetenzzentrum für elektronische Erschließungs- und Publikationsverfahren in den Geisteswissenschaften des Fachbereichs Sprach-, Literatur- und Medienwissenschaften.